

Vigor2910 Dual-WAN Security Router User's Guide

Version: 3.2

Date: 2007/10/01

Copyright 2007 All rights reserved.

This publication contains information that is protected by copyright. No part may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language without written permission from the copyright holders. The scope of delivery and other details are subject to change without prior notice.

Microsoft is a registered trademark of Microsoft Corp. Windows, Windows 95, 98, Me, NT, 2000, XP and Explorer are trademarks of Microsoft Corp. Apple and Mac OS are registered trademarks of Apple Computer Inc. Other products may be trademarks or registered trademarks of their respective manufacturers.

Table of Contents



Preface	.1
1.1 Web Configuration Buttons Explanation	. 1
1.2 LED Indicators and Connectors	. 1
1.2.1 For Vigor2910 1.2.2 For Vigor2910G 1.2.3 For Vigor2910i 1.2.4 For Vigor2910V 1.2.5 For Vigor2910VG 1.2.6 For Vigor2910VG.	. 3 . 4 . 5
1.3 Hardware Installation	
1.4 Printer Installation	9



Configuring Basic Settings	15
2.1 Changing Password	15
2.2 Quick Start Wizard	17
2.2.1 PPPoE 2.2.2 PPTP 2.2.3 Static IP 2.2.4 L2TP 2.2.5 DHCP	
2.3 Online Status	24
2.4 Saving Configuration	26



Advanced Web Configuration	27
3.1 WAN	
 3.1.1 Basics of Internet Protocol (IP) Network 3.1.2 Network Connection by 3G USB Modem	
3.2 LAN	
3.2.1 Basics of LAN3.2.2 General Setup3.2.3 Static Route3.2.4 Bind IP to MAC	
3.3 NAT	50
3.3.1 Port Redirection 3.3.2 DMZ Host 3.3.3 Open Ports	

3.4 Objects and Groups	57
3.4.1 IP Object 3.4.2 IP Group	59
3.4.3 Service Type Object	
3.4.4 Service Type Group 3.4.5 CSM Profile	
3.5 Firewall	
3.5.1 Basics for Firewall	
3.5.2 General Setup 3.5.3 Filter Setup	
3.5.4 DoS Defense	
3.5.5 URL Content Filter	
3.5.6 Web Content Filter	79
3.6 Bandwidth Management	80
3.6.1 Sessions Limit	80
3.6.2 Bandwidth Limit	
3.6.3 Quality of Service	82
3.7 Applications	89
3.7.1 Dynamic DNS	89
3.7.2 Schedule	91
3.7.3 RADIUS	
3.7.4 UPnP 3.7.5 Wake On LAN	
3.8 VPN and Remote Access	
3.8.1 Remote Access Control	
3.8.2 PPP General Setup 3.8.3 IPSec General Setup	
3.8.4 IPSec Peer Identity	
3.8.5 Remote Dial-in User	
3.8.6 LAN to LAN	
3.8.7 VPN TRUNK Management	
3.8.8 Connection Management	
3.9 Certificate Management	
3.9.1 Local Certificate	
3.9.2 Trusted CA Certificate 3.9.3 Certificate Backup	
3.10 VoIP	
3.10.1 DialPlan	
3.10.2 SIP Accounts	
3.10.3 Phone Settings 3.10.4 Status	
3.11 ISDN	
3.11.1 General Setup 3.11.2 Dialing to a Single ISP	
3.11.3 Dialing to Dual ISPs	
3.11.4 Virtual TA	
3.11.5 Call Control	
3.12 Wireless LAN	. 151
3.12.1 Basic Concepts	. 151
3.12.2 General Settings	. 154
3.12.3 Security	. 156

3.12.4 Access Control	
3.12.5 WDS	159
3.12.6 AP Discovery	161
3.12.7 Station List	
3.12.8 Station Rate Control	163
3.13 VLAN	
3.13.1 Wired VLAN	
3.13.2 Wireless VLAN	
3.13.3 VLAN Cross Setup	
3.13.4 Wireless Rate Control	169
3.14 System Maintenance	170
3.14.1 System Status	170
3.14.2 TR-069 Setting	
3.14.3 Administrator Password	
3.14.4 Configuration Backup	
3.14.5 Syslog/Mail Alert	
3.14.6 Time and Date	176
3.14.7 Management	177
3.14.8 Reboot System	178
3.14.9 Firmware Upgrade	179
3.15 Diagnostics	180
3.15.1 Dial-out Trigger	
3.15.2 Routing Table	
3.15.3 ARP Cache Table	
3.15.4 DHCP Table	
3.15.5 NAT Sessions Table	
3.15.6 Wireless VLAN Online Station Table	
3.15.7 Data Flow Monitor	
3.13.8 Traffic Graph	
3.15.9 Ping Diagnosis	
3.15.10 Trace Route	



Application and Examples1	189
4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter	189
4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter	196
4.3 QoS Setting Example	200
4.4 LAN – Created by Using NAT	202
4.5 Calling Scenario for VoIP function	204
4.5.1 Calling via SIP Sever 4.5.2 Peer-to-Peer Calling	
4.6 Upgrade Firmware for Your Router	207
4.7 Request a certificate from a CA server on Windows CA Server	209
4.8 Request a CA Certificate and Set as Trusted on Windows CA Server	213
4.9 VPN TRUNK Application	215
4.10 ERD Mechanism for VPN TRUNK	219



Trouble Shooting	221
5.1 Checking If the Hardware Status Is OK or Not	221
5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not	221
5.3 Pinging the Router from Your Computer	224
5.4 Checking If the ISP Settings are OK or Not	226
5.5 Problems for 3G Network Connection	227
5.6 Backing to Factory Default Setting If Necessary	228
5.7 Contacting Your Dealer	229



The Vigor2910 series router provides Dual-WAN interface (which is a configuration second WAN) for Internet access to make the Internet connection more reliable. The wireless LAN supports more secure features and the transmission speed is up to 108Mbps (SuperGTM). Object-oriented firewall is flexible and allows your network be safe. In addition, through VoIP function, the communication fee for you and remote people can be reduced.

1.1 Web Configuration Buttons Explanation

Several main buttons appeared on the web pages are defined as the following:

OK	Save and apply current settings.
Cancel	Cancel current settings and recover to the previous saved settings.
Clear	Discard current settings and allow users to input settings again.
Add	Add new settings for specified item.
Edit	Edit the settings for the selected item.
Delete	Delete the selected item with the corresponding settings.
Note: For th	e other buttons shown on the web pages, please refer to Chapter 4 for

detailed explanation.

1.2 LED Indicators and Connectors

Before you use the Vigor router, please get acquainted with the LED indicators and connectors first.

The displays of LED indicators and connectors for the routers are different slightly. The following sections will introduce them respectively.

1.2.1 For Vigor2910

LED Explanation

ACT DMZ QoS Attack VPN US	B W1 W2/P1 P2 P3 P4	

LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation



Interface	Description
USB*	Connecter for a USB printer or 3G USB modem.
PWR	Connecter for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
LAN P4 – P1	Connecters for local networked devices.
W2/W1	Connecter for accessing Internet with the ADSL, ADSL2/2+ line
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

1.2.2 For Vigor2910G

LED Explanation

							/						
					и	/A N	LA	N					
ACT	DMZ	QoS	Attack	WLAN USB		W2/P1			P4				

LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
WLAN	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
	Off	Wireless access point is turned off.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3,	Orange	A normal 10Mbps connection is through its corresponding
P4)	-	port.
,	Green	A normal 100Mbps connection is through its
		corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation



Interface	Description
USB*	Connecter for a USB printer or 3G USB modem.
PWR	Connecter for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
LAN P4 – P1	Connecters for local networked devices.
W2/W1	Connecter for accessing Internet with the ADSL, ADSL2/2+ line
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

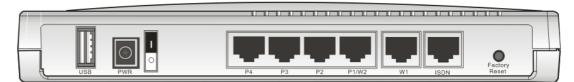
1.2.3 For Vigor2910i

LED Explanation

			WA N	LAN		
ACT I	SDN QoS Attack	VPN USB	W1 W2/P1	P2	P3 P4	

LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful connection on the ISDN BRI B1/B2 channel.
QoS	On	The QoS function is active.
	Off	The QoS function is inactive.
Attack	On	DoS Defense function is active.
	Blinking	An attack is detected.
VPN	On	The VPN tunnel is launched.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2,	Orange	A normal 10Mbps connection is through its corresponding
P3, P4)		port.
	Green	A normal 100Mbps connection is through its corresponding
		port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation



Interface	Description
USB*	Connecter for a USB printer or 3G USB modem.
PWR	Connecter for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
LAN P4 – P1	Connecters for local networked devices.
W2/W1	Connecter for accessing Internet with the ADSL, ADSL2/2+ line
ISDN	Connecter for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

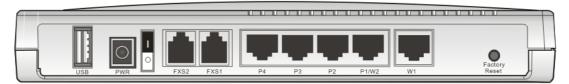
1.2.4 For Vigor2910V

LED Explanation

				_	_	/
	FXS1 FXS2	USB	WAN W1 W2/P1	P2	N P3	P4

LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
FXS1/FXS2	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming or on-line.
VPN	On	The VPN tunnel is launched.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2, P3, P4)	Orange	A normal 10Mbps connection is through its corresponding port.
	Green	A normal 100Mbps connection is through its corresponding port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation



Interface	Description
USB*	Connecter for a USB printer or 3G USB modem.
PWR	Connecter for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
FXS2 & FXS1	Connecters for telephone set and analog phone with VoIP communication.
LAN P4 - P1	Connecters for local networked devices.
W2/W1	Connecter for accessing Internet with the ADSL, ADSL2/2+ line
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

1.2.5 For Vigor2910VG

LED Explanation

LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
DMZ	On	DMZ Host is specified in certain site.
FXS1/FXS2	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming or on-line.
WLAN	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
	Off	Wireless access point is turned off.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2,	Orange	A normal 10Mbps connection is through its corresponding
P3, P4)		port.
	Green	A normal 100Mbps connection is through its corresponding
		port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation

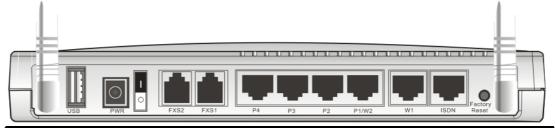
	PWR C FXS2 FXS1 P4 P3 P2 P1/W2 W1 Reset					
Interface	Description					
USB*	Connecter for a USB printer or 3G USB modem.					
PWR	Connecter for a power adapter with 12-15VDC.					
ON/OFF	Power Switch.					
FXS2 & FXS1	Connecters for telephone set and the analog phone with VoIP communication.					
LAN P4 – P1	Connecters for local networked devices.					
W2/W1	Connecter for accessing Internet with the ADSL, ADSL2/2+ line					
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.					

1.2.6 For Vigor2910VGi

LED Explanation

107 1001	Phone FXS1 FXS2 WLAN U	WAN LAN
	FXS1 FXS2 WLAN U	ISB W1 W2/P1 P2 P3 P4
LED	Status	Explanation
ACT (Activity)	Blinking	The router is powered on and running properly.
	Off	The router is powered off.
ISDN	On	The ISDN network is correctly setup.
	Blinking	A successful connection on the ISDN BRI B1/B2 channel.
FXS1/FXS2	On	The phone is off hook (the handset of phone is hanging).
	Blinking	A phone call is incoming or on-line.
WLAN	On	Wireless access point is ready.
	Blinking	Wireless traffic goes through.
	Off	Wireless access point is turned off.
USB *	On	The USB interface printer or 3G USB modem is ready.
WAN(W1-W2)	Orange	A normal 10Mbps WAN link is ready.
	Green	A normal 100Mbps WAN link is ready.
	Blinking	Ethernet packets are transmitting.
LAN (P1, P2,	Orange	A normal 10Mbps connection is through its corresponding
P3, P4)		port.
	Green	A normal 100Mbps connection is through its corresponding
		port.
	Blinking	Ethernet packets are transmitting.

Connector Explanation



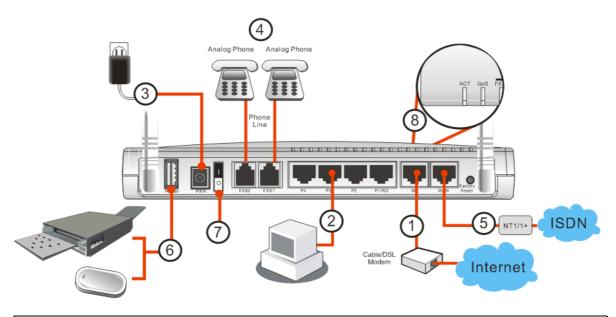
Interface	Description
USB*	Connecter for a USB printer or 3G USB modem.
PWR	Connecter for a power adapter with 12-15VDC.
ON/OFF	Power Switch.
FXS2 & FXS1	Connecters for telephone set and analog phone with VoIP communication.
LAN P4 - P1	Connecters for local networked devices.
W2/W1	Connecter for accessing Internet with the ADSL, ADSL2/2+ line
ISDN	Connecter for NT1 (or NT1+) box provided by ISDN service provider.
Factory Reset	Restore the default settings. Usage: Turn on the router (ACT LED is blinking). Press the hole and keep for more than 5 seconds. When you see the ACT LED begins to blink rapidly than usual, release the button. Then the router will restart with the factory default configuration.

1.3 Hardware Installation

Before starting to configure the router, you have to connect your devices correctly.

- 1. Connect this device to a router/modem with an Ethernet cable.
- 2. Connect one port of 4-port switch to your computer with a RJ-45 cable. This device allows you to connect 4 PCs directly.
- 3. Connect one end of the power cord to the power port of this device. Connect the other end to the wall outlet of electricity.
- 4. Connect the telephone sets with phone lines (for using VoIP function). For the user of the model without VoIP ports, skip this step.
- 5. Connect the ISDN NT1/1+ box with ISDN cable. This connection is available for Europe only.
- 6. Connect the printer/3.5G modem (e.g., Huawei E220 HSDPA USB Modem) to the router with the USB cable and connect the power cord if requried. If you do not have a printer/3.5G modem for using, skip this step. For detailed configuration of printer, refer to section 1.4; detailed configuration of 3.5G modem, please refer to section 3.1.
- 7. Power on the router.
- 8. Check the ACT LED to assure network connections.

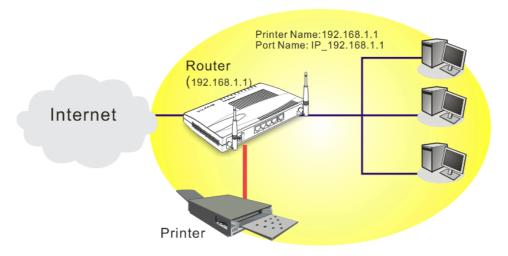
(For the detailed information of LED status, please refer to section 1.1.)



Caution: Each of the FXS ports can be connected to an analog phone only. Do not connect the FXS ports to the telephone wall jack. This connection might damage your router.

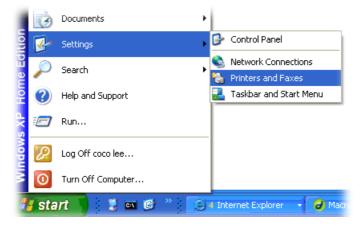
1.4 Printer Installation

You can install a printer onto the router for sharing printing. All the PCs connected this router can print documents via the router. The example provided here is made based on Windows XP/2000. For Windows 98/SE, please visit www.draytek.com.



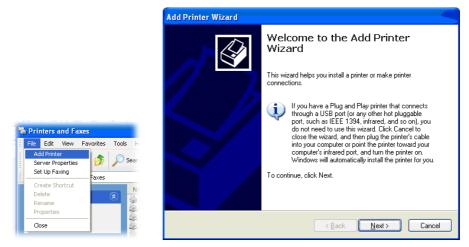
Before using it, please follow the steps below to configure settings for connected computers (or wireless clients).

1. Connect the printer with the router through USB/parallel port.

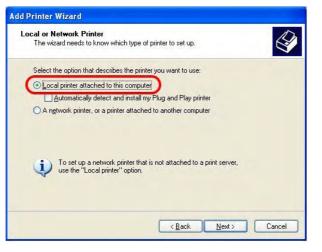


2. Open Start->Settings-> Printer and Faxes.

3. Open File->Add a New Computer. A welcome dialog will appear. Please click Next.



4. Click Local printer attached to this computer and click Next.



5. In this dialog, choose **Create a new port Type of port** and use the drop down list to select **Standard TCP/IP Port**. Click **Next**.

lect a Printer Port Computers communicate w	with printers through ports.	
Select the port you want yo new port.	our printer to use. If the port is not listed, you	can create a
OUse the following port:	LPT1: (Recommended Printer Port)	192
60		
		-

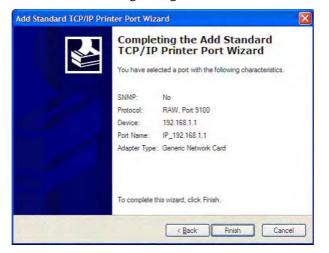
6. In the following dialog, type **192.168.1.1** (router's LAN IP) in the field of **Printer** Name or IP Address and type IP_192.168.1.1 as the port name. Then, click Next.

dd Port For which device do you wan	t to add a port?
Enter the Printer Name or IP a	ddress, and a port name for the desired device.
Printer Name or IP <u>A</u> ddress:	192.168.1.1
Port Name:	IP_192.168.1.1

7. Click Standard and choose Generic Network Card.

A	dd Standard TCP/IP Printer Port Wizard 🛛 🔀
	Additional Port Information Required The device could not be identified.
	The detected device is of unknown type. Be sure that: 1. The device is properly configured. 2. The address on the previous page is correct.
	Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.
	Device Type
	O Eustom
	< <u>Back</u> <u>N</u> ext>Cancel

8. Then, in the following dialog, click **Finish**.



9. Now, your system will ask you to choose right name of the printer that you installed onto the router. Such step can make correct driver loaded onto your PC. When you finish the selection, click **Next**.

The manuracturer	and model determine which printer software to use	17
	ufacturer and model of your printer. If your printer ca e Disk. If your printer is not listed, consult your printe	
compatible prin		
Manufacturer	Printers	1
AST AT&T	Brother HL-1060 BR-Script2	
Brother	Brother HL-1070 BR-Script2	
Buil	Brother HL-1070	
Canon		
This driver is digitally	signed. Windows Updat	e <u>H</u> ave Disk
	igning is important	

10. For the final stage, you need to go back to **Control Panel-> Printers** and edit the property of the new printer you have added.

eneral Sha	ring Ports	Advanced	Device Se	ettings	
Br	other HL-1070				
~~	_				_
	allowing port(s).	Documents	will print to	the first free	
checked por	t.		_		
Port	Description		Printer		3
3.250	Standard TCF	VIP Port	Epson Stylu	IS COLOR 1160	
□ IP_1	Standard TCF	P/IP Port			
□ IP_1	Standard TCF	VIP Port	HP LaserJe	t1300	
□ IP_1	Standard TCF	P/IP Port			
	Standard TCF				
	Standard TCF		Brother HL-	1070	
D PDF	Local Port		PDF995	_	1
Add P	ort	Delete I	Port	Configure Port	E.v.
Theat		<u>_</u>			
Enable bi	directional supp	10			
Enable pr	inter pooling				

11. Select "LPR" on Protocol, type **p1** (number 1) as Queue Name. Then click **OK**. Next please refer to the red rectangle for choosing the correct protocol and UPR name.

onfigure Standard TCP/I	P Port Monitor	?
Port Settings		-
Port Name:	IP_192.168.1.1	
Printer Name or IP Address:	192.168.1.1	
Protocol O <u>R</u> aw		D
- Raw Settings		
Port Number 91	00	
LPR Settings Queue Name: p1	1	1
LPR Byte Counting Enab	aled	
SNMP Status Enabled		
Community Name: pu	iblic	
SNMP Device Index:		
	OK	Cancel

The printer can be used for printing now. Most of the printers with different manufacturers are compatible with vigor router.

Note 1: Some printers with the fax/scanning or other additional functions are not supported. If you do not know whether your printer is supported or not, please visit www.draytek.com to find out the printer list. Open **Support Center->FAQ->Sort by product**; select the model of the router and click on it; find out the link of **Printer Server FAQ**; click the **What types of printers are compatible with Vigor router**? link.



Note 2: Vigor router supports printing request from computers via LAN ports but not WAN port.

2 Configuring Basic Settings

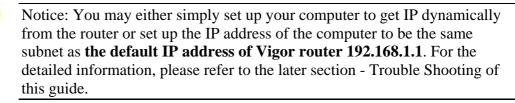
For use the router properly, it is necessary for you to change the password of web configuration for security and adjust primary basic settings.

This chapter explains how to setup a password for an administrator and how to adjust basic settings for accessing Internet successfully. Be aware that only the administrator can change the router configuration.

2.1 Changing Password

To change the password for this device, you have to access into the web browse with default password first.

1. Make sure your computer connects to the router correctly.



2. Open a web browser on your PC and type http://192.168.1.1. A pop-up window will open to ask for username and password. Please type default values (both username and password are Null) on the window for the first time accessing and click **OK** for next screen.



3. Now, the **Main Screen** will pop up. Notice that the main screen differs according to the model of the router that you have. Below is an example.

Vigor291 Dual-WAN Security	O Series	BA		15	DrayTek www.draytek.com
Quick Start Wizard	System Status				
Online Status	Model Name Firmware Version	: DrayTek Vigor2 : 3.1.0			
WAN	Build Date/Time	: Fri Aug 17 16:39	9:16.11 2007		
LAN NAT		System			WAN 1
Firewall	CPU Usage	:4%		Link Status	: Connected
	Total Memory	: 16M		MAC Address	: 00-50-7F-DD-15-19
Objects and Groups	Memory usage	: 60 %		Connection	: Static IP
Bandwidth Management				IP Address	: 172.16.3.229 : 172.16.3.4
Applications		LAN		Default Gateway	: 172.10.3.4
VPN and Remote Access	MAC Address	: 00-50-7F-			reless I AN
Certificate Management	1st IP Address	: 192.168.1			
VoIP	1st Subnet Mask DHCP Server	: 255.255.2 : Yes	55.0	MAC Address	: 00-14-85-08-69-19
ISDN	DHCP Server	: Yes : 194.109.6	<i>c c</i>	Frequency Domain Firmware Version	: Europe : v2.01.10.10.5.4
Wireless LAN	DNS	: 194.109.0	.00	Firmware version	: v2.01.10.10.5.4
VIAN		VolP			
System Maintenance	Port	: 1	2		
Diagnostics	SIP registrar	. 1	2		
All Rights Reserved.	Account ID	: change_me	change_me		
-	Register	:			
	Codec	:			
	In Calls	: 0	0		
	Out Calls	: 0	0		

4. Go to **System Maintenance** page and choose **Administrator Password**.

System Maintenance >> Administrator Password Setup

Old Password	
New Password	
Confirm Password	

- 5. Enter the login password (the default is blank) on the field of **Old Password**. Type a new one in the field of **New Password** and retype it on the field of **Retype New Password**. Then click **OK** to continue.
- 6. Now, the password has been changed. Next time, use the new password to access the Web Configurator for this router.

Connect to 192.1	68.1.1	? 🔀
Login to the Router	Web Configurator	
User name:	2	~
Password:	••••	
	Remember my pass	sword
	ОК	Cancel

2.2 Quick Start Wizard

If your router can be under an environment with high speed NAT, the configuration provide here can help you to deploy and use the router quickly. The first screen of Quick Start Wizard is entering login password. After typing the password, please click Next.

Quick Start Wizard	
Enter login password	
Please enter an alpha-numeric s	string as your Password (Max 23 characters).
New Password	••••
Confirm Password	••••
	< Back Next > Finish Cancel

On the next page as shown below, please select the WAN interface that you use. Choose Auto negotiation as the physical type for your router. Then click Next for next step.

Quick Start Wizard

Select WAN Interface		
Select WAN Interface: Display Name: Physical Mode: Physical Type:	WAN1 Ethemet Auto negotiation Auto negotiation 10M half duplex 10M full duplex 100M half duplex 100M full duplex	
	< Back Next > Finish C	ancel

On the next page as shown below, please select the appropriate Internet access type according to the information from your ISP. For example, you should select PPPoE mode if the ISP provides you PPPoE interface. Then click **Next** for next step.

Quick S	tart	Wiz	ard
---------	------	-----	-----

Connee	ct to Internet
	WAN 1
	Select one of the following Internet Access types provided by your ISP.
	PPPoE
	○ РРТР
	◯ L2TP
	Static IP
	O DHCP
	<pre>< Back Next > Finish Cancel</pre>

In the **Quick Start Wizard**, you can configure the router to access the Internet with different protocol/modes such as **PPPoE**, **PPTP**, **L2TP**, **Static IP** or **DHCP**. The router supports the DSL WAN interface for Internet access.

2.2.1 PPPoE

PPPoE stands for **Point-to-Point Protocol over Ethernet**. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

If your ISP provides you the **PPPoE** connection, please select **PPPoE** for this router. The following page will be shown: Quick Start Wizard

PPPoE Client Mode	
WAN 1	
Enter the user name and pa	ssword provided by your ISP.
User Name	84005755@hinet.net
Password	•••••
Confirm Password	•••••
	<pre>< Back Next > Finish Cancel</pre>

User Name Assign a specific valid user name provided by the ISP.

Password Assign a valid password provided by the ISP.

Confirm Password Retype the password for confirmation.

Click Next for viewing summary of such connection.

Quick Start Wizard

ase confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	PPPoE
settings and restart the V	
	< Back Next > Finish Canc

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.2.2 PPTP

Click **PPTP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard

WAN 1	
Enter the user name, pas your ISP.	word, WAN IP configuration and PPTP server IP provided by
User Name	
Password	
Confirm Password	
WAN IP Configuration	
🔘 Obtain an IP addres	automatically
💿 Specify an IP addre	;
IP Address	172.16.3.229
Subnet Mask	255.255.0.0
PPTP Server IP	

Click Next for viewing summary of such connection.

Quick	Start	Wizard
-------	-------	--------

WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	РРТР
	nges if necessary. Otherwise, click Finish to save the current
Click Back to modify char settings and restart the V	

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.2.3 Static IP

Click **Static IP** as the protocol. Type in all the information that your ISP provides for this protocol.

Quick Start Wizard		
Static IP Client Mode		
WAN 1 Enter the Static IP config	uration probided by your ISP.	
WAN IP	172.16.3.229	
Subnet Mask	255.255.255.0	
Gateway	172.16.3.1	
Primary DNS	168.95.1.1	
Secondary DNS		(optional)
	< Back	Next > Finish Cancel

After finishing the settings in this page, click **Next** to see the following page.

Quick Start Wizard

Please confirm your settings:	
WAN Interface: Physical Mode: Physical Type:	WAN1 Ethernet Auto negotiation
Internet Access:	Static IP
Click Back to modify chan settings and restart the Vi	ges if necessary. Otherwise, click Finish to save the current gor router.
	< Back Next > Finish Cancel

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.2.4 L2TP

Click L2TP as the protocol. Type in all the information that your ISP provides for this protocol. Quick Start Wizard

WAN 1 Enter the user name, pass	word, WAN IP configuration and L2TP server IP provided by
your ISP.	
User Name	
Password	
Confirm Password	
WAN IP Configuration	
🔘 Obtain an IP address	automatically
Specify an IP addres:	
IP Address	172.16.3.229
Subnet Mask	255.255.0.0
L2TP Server IP	

After finishing the settings in this page, click **Next** to see the following page.

Quick Start Wizard

Please confirm your settings:	
WAN Interface: Physical Mode: Physical Type: Internet Access:	WAN1 Ethernet Auto negotiation
	L2TP nges if necessary. Otherwise, click Finish to save the current rigor router.
	< Back Next > Finish Cancel

Click **Finish.** A page of **Quick Start Wizard Setup OK!!!** will appear. Then, the system status of this protocol will be shown.

2.2.5 DHCP

Click **DHCP** as the protocol. Type in all the information that your ISP provides for this protocol. Quick Start Wizard

Quick Start Wizard

WAN 1 If your ISP req enter it in.	uire you to enter a specific host name or specific MAC address, please
Host Name MAC	(optional) 00 -50 -7F -00 -00 -01 (optional)

After finishing the settings in this page, click **Next** to see the following page.

Please confirm your settings:	
WAN Interface:	WAN1
Physical Mode:	Ethernet
Physical Type:	Auto negotiation
Internet Access:	DHCP
Click Back to modify char	iges if necessary. Otherwise, click Finish to save the current
settings and restart the V	igor router.
	< Back Next > Finish Cancel

Click Finish. A page of Quick Start Wizard Setup OK !!! will appear. Then, the system status of this protocol will be shown.

2.3 Online Status

The online status shows the system status, WAN status, ADSL Information and other status related to this router within one page. If you select **PPPoE** as the protocol, you will find out a button of **Dial PPPoE** or **Dial PPPoE** in the Online Status web page.

Online status for PPPoE

Online Status

System Status					System Uptime: 0:0:41
LAN Status		Primary DNS: 61.31.233.1		Secondary D	NS: 139.175.55.244
IP Address	TX Pack	cets F	X Packets		
192.168.50.111	L 240	2	210		
WAN 1 Status					>> <u>Drop PPPoE</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:00:00	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
219.81.160.205	5 211.78.218.40	6	29	6	12
WAN 2 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		Static IP	0:00:32	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.4.103	192.168.4.1	1	3	1	9

Online status for PPTP (for WAN2)

Online Status

LAN Status		Primary DNS:	194.109.6.66	Secondary	DNS: 194.98.0.1
IP Address	TX Pack	ets	RX Packets		
192.168.50.111	4910		3663		
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN1	Static IP	0:10:08	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.22.111	192,168,22,105	91	21	99	3
WAN 2 Status					>> <u>Drop PPT</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.29.202	192.168.29.1	103	119	14	6

Online status for Static IP(for WAN1)

Online Status

LAN Status		Primary DNS:	194.109.6.66	Secondary	DNS: 194.98.0.1
IP Address	TX Pack	tets	RX Packets		
192.168.50.111	4910		3663		
WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN1	Static IP	0:10:08	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192,168,22,111	192,168,22,105	91	21	99	3
WAN 2 Status					>> <u>Drop PPT</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet	WAN2	PPTP	0:00:15	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192.168.29.202	192.168.29.1	103	119	14	6

Online status for DHCP

Online Status

LAN Status		Primary DNS:	168.95.1.1	Secondary	DNS: 168.95.1.1
IP Address	TX Pack	cets F	RX Packets		
192.168.50.111	1 856	7	/83		
WAN 1 Status					>> <u>Release</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		DHCP Client	0:01:49	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
192,168,22,10	192,168,22,105	3	З	7	9
WAN 2 Status					>> <u>Drop PPPoE</u>
Enable	Line	Name	Mode	Up Time	
Yes	Ethernet		PPPoE	0:01:39	
IP	GW IP	TX Packets	TX Rate	RX Packets	RX Rate
202.211.100.17	76 202.211.100.17	70 35	8	46	4

Detailed explanation is shown below:

Primary DNS	Displays the IP address of the primary DNS.
Secondary DNS	Displays the IP address of the secondary DNS.
LAN Status	
IP Address	Displays the IP address of the LAN interface.
TX Packets	Displays the total transmitted packets at the LAN interface.
RX Packets	Displays the total number of received packets at the LAN interface.
WAN1/2 Status	
Line	Displays the physical connection (Ethernet) of this interface.
Name	Displays the name set in WAN1/WAN web page.
Mode	Displays the type of WAN connection (e.g., PPPoE).
Up Time	Displays the total uptime of the interface.
IP	Displays the IP address of the WAN interface.
GW IP	Displays the IP address of the default gateway.
TX Packets	Displays the total transmitted packets at the WAN interface.
TX Rate	Displays the speed of transmitted octets at the WAN interface.
RX Packets	Displays the total number of received packets at the WAN interface.
RX Rate	Displays the speed of received octets at the WAN interface.
	een mean that the WAN connection of that interface

(WAN1/WAN2) is ready for accessing Internet; the words in red mean that the WAN connection of that interface (WAN1/WAN2) is not ready for accessing Internet.

2.4 Saving Configuration

Each time you click **OK** on the web page for saving the configuration, you can find messages showing the system interaction with you.

Status: Settings Saved

Ready indicates the system is ready for you to input settings.

Settings Saved means your settings are saved once you click Finish or OK button.



After finished basic configuration of the router, you can access Internet with ease. For the people who want to adjust more setting for suiting his/her request, please refer to this chapter for getting detailed information about the advanced configuration of this router. As for other examples of application, please refer to chapter 4.

3.1 WAN

Quick Start Wizard offers user an easy method to quick setup the connection mode for the router. Moreover, if you want to adjust more settings for different WAN modes, please go to **WAN** group and click the **Internet Access** link.

3.1.1 Basics of Internet Protocol (IP) Network

IP means Internet Protocol. Every device in an IP-based Network including routers, print server, and host PCs, needs an IP address to identify its location on the network. To avoid address conflicts, IP addresses are publicly registered with the Network Information Centre (NIC). Having a unique IP address is mandatory for those devices participated in the public network but not in the private TCP/IP local area networks (LANs), such as host PCs under the management of a router since they do not need to be accessed by the public. Hence, the NIC has reserved certain addresses that will never be registered publicly. These are known as *private* IP addresses, and are listed in the following ranges:

From 10.0.0.0 to 10.255.255.255 From 172.16.0.0 to 172.31.255.255 From 192.168.0.0 to 192.168.255.255

What are Public IP Address and Private IP Address

As the router plays a role to manage and further protect its LAN, it interconnects groups of host PCs. Each of them has a private IP address assigned by the built-in DHCP server of the Vigor router. The router itself will also use the default **private IP** address: 192.168.1.1 to communicate with the local hosts. Meanwhile, Vigor router will communicate with other network devices through a **public IP** address. When the data flow passing through, the Network Address Translation (NAT) function of the router will dedicate to translate public/private addresses, and the packets will be delivered to the correct host PC in the local area network. Thus, all the host PCs can share a common Internet connection.

Get Your Public IP Address from ISP

In ADSL deployment, the PPP (Point to Point)-style authentication and authorization is required for bridging customer premises equipment (CPE). Point to Point Protocol over Ethernet (PPPoE) connects a network of hosts via an access device to a remote access concentrator or aggregation concentrator. This implementation provides users with significant ease of use. Meanwhile it provides access control, billing, and type of service according to user requirement.

When a router begins to connect to your ISP, a serial of discovery process will occur to ask for a connection. Then a session will be created. Your user ID and password is authenticated via **PAP** or **CHAP** with **RADIUS** authentication system. And your IP address, DNS server, and other related information will usually be assigned by your ISP.

3.1.2 Network Connection by 3G USB Modem

For 3G mobile communication through Access Point is popular more and more, Vigor 2910 adds the function of 3G network connection for such purpose. By connecting 3G USB Modem to the USB port of Vigor2910, it can support HSDPA/UMTS/EDGE/GPRS/GSM and the future 3G standard (HSUPA, etc). Vigor2910 with 3G USB Modem allows you to receive 3G signals at any place such as your car or certain location holding outdoor activity and share the bandwidth for using by more people. Users can use four LAN ports on the router to access Internet. Also, they can access Internet via SuperG wireless function of Vigor2910G, and enjoy the powerful firewall, bandwidth management, VPN, VoIP features of Vigor2910 series.



After connecting into the router, 3G USB Modem will be regarded as the second WAN port. However, the original Ethernet WAN1 still can be used and Load-Balance can be done in the router. Besides, 3G USB Modem in WAN2 also can be used as backup device. Therefore, when WAN1 is not available, the router will use 3.5G for supporting automatically. The supported 3G USB Modem will be listed on Draytek web site. Please visit www.draytek.com for more detailed information.

Below shows the menu items for Internet Access.



3.1.3 General Setup

This section will introduce some general settings of Internet and explain the connection modes for WAN1 and WAN2 in details.

This router supports dual WAN function. It allows users to access Internet and combine the bandwidth of the dual WAN to speed up the transmission through the network. Each WAN port (WAN1- through WAN port/WAN2- through LAN1 port) can connect to different ISPs, Even if the ISPs use different technology to provide telecommunication service (such as DSL, Cable modem, etc.). If any connection problem occurred on one of the ISP connections, all the traffic will be guided and switched to the normal communication port for proper operation. Please configure WAN1 and WAN2 settings.

This webpage allows you to set general setup for WAN1 and WAN respectively.

Note: In default, WAN1 is enabled. WAN2 is optional.

WAN >> General Setup

General Setup			
WAN1		WAN2	
Enable:	Yes 💙	Enable:	Yes 🕶
Display Name:		Display Name:	
Physical Mode:	Ethernet	Physical Mode:	Ethernet 🔽
Physical Type:	Auto negotiation 👻	Physical Type:	Ethernet
Load Balance Mode:	Auto Weight 🔽	Load Balance Mode:	3G USB Modem
Line Speed(Kbps):	DownLink 🛛	Line Speed(Kbps):	DownLink D
	UpLink 🛛		UpLink
Active Mode:	Always On 🛛 👻	Active Mode:	Always On 🔽
Active on demand:		Active on demand:	
🔿 WAN2 Fail		🔿 WAN1 Fail	
WAN2 Upload spe	ed exceed C Kbps	WAN1 Upload spe	ed exceed 🛛 Kbps
WAN2 Download	speed exceed OKbps	WAN1 Download :	speed exceed OKbps

Note: WAN2 and LAN P1 share the P1 port. When WAN2 is enabled, P1 is used as WAN2.

Physical Type:

OK

Enable	Choose Yes to invoke the settings for this WAN interface. Choose No to disable the settings for this WAN interface.			
Display Name	Type the description for the WAN1/WAN2 interface.			
Physical Mode	For WAN1, the physical connection is done and fixed Ethernet port; yet the physical connection for WAN2 through an Ethernet port (P1) or USB port. You canno change it.			
	Physical Mode:	Ethernet Ethernet 3G USB Modem		

To use 3G network connection through 3G USB Modem, choose **3G USB Modem** as the physical mode in **WAN2**. Next, go to **WAN>> Internet Access**. 3G USB Modem is available for WAN2. You can choose **PPP** as the access mode and click Details Page for further configuration.

nternet Access			
Index Display Name	Physical Mode	Access Mode	
WAN1	Ethernet	Static or Dynamic IP 🔽 🛛 Details	s Page
/AN2	3G USB Modem	None 🔽 Details	s Page
		None	

Physical Type

You can change the physical type for WAN2 or choose **Auto negotiation** for determined by the system.

Auto negotiation	*
Auto negotiation	
10M half duplex	
10M full duplex	
100M half duplex 100M full duplex	
100M full duplex	

Load Balance Mode	please choose the setting of	bandwidth for your WAN interface, of According to Line Speed . Auto Weigh to let the router reach
	Load Balance Mode:	Auto Weigh Auto Weigh According to Line Speed
Line Speed	Balance Mode, please typ	g to Line Speed as the Load be the line speed for downloading AN1/WAN2. The unit is kbps.
Active Mode		tivated always; or choose Active on N connection (WAN1/WAN2)
	Active Mode:	Active on demand 👻 Always On Active on demand
	available for you to set for the Details Page of WAN2 are three selections for yo WAN2 Fail – It means th activated when WAN2 is WAN2 Upload speed exc connection for WAN1 will speed exceed certain value seconds. WAN2 Download speed connection for WAN1 will Download speed exceed c for 15 seconds. WAN1 Fail – It means th activated when WAN1 is WAN1 Upload speed exc connection for WAN2 will speed exceed certain value seconds. WAN1 Download speed connection for WAN2 will speed exceed certain value	ceed XX kbps – It means the Il be activated when WAN2 Upload e that you set in this box for 15 exceed XX kbps – It means the Il be activated when WAN2 certain value that you set in this box e connection for WAN2 will be

3.1.4 Internet Access

For the router supports dual WAN function, the users can set different WAN settings (for WAN1/WAN2) for Internet Access. Due to different Physical Mode for WAN1 and WAN2, the Access Mode for these two connections also varies slightly.

nternet Access		
Index Display Name	Physical Mode	Access Mode
WAN1	Ethernet	Static or Dynamic IP 💌 🛛 Details Page
WAN2	3G USB Modem	None 💌 Details Page
		None PPP

WAN >> Internet Access

WAN >> Internet Access

Index Display Name	Physical Mode	Access Mode
WAN1	Ethernet	Static or Dynamic IP 👻 🛛 Details Page
WAN2	Ethernet	None
1		None PPPoE Static or Dynamic IP PPTP/L2TP
Index	default WAN in the optional WA	N modes that this router supports. WAN1 is the terface for accessing into the Internet. WAN2 is N interface for accessing into the Internet when we for some reason.
Display Name	It shows the nam setup.	e of the WAN1/WAN2 that entered in general
Physical Mode		sical connection for WAN1 (Ethernet) /WAN2USB Modem) according to the real networkPhysical Mode
	Ethernet	Ethernet
	3G USB Mode	m Ethernet
Access Mode	page of that mod	wn list to choose a proper access mode. The detai le will be popped up. If not, click Details Page fo ge to configure the settings.
	Static or Dynan None PPPoE Static or Dynam PPTP/L2TP	
	There are three a Dynamic IP and	ccess modes provided for PPPoE, Static or PPTP/L2TP.
Details Page		open different web page according to the access noose in WAN1 or WAN2.

Details Page for PPPoE

To use **PPPoE** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPPoE** mode for WAN2. The following web page will be shown.

W/AN	>>	Internet	Access
WAN	22	internet	Access

PPPoE Client Mode		PPP/MP Setup
🔘 Enable 🛛 💿 Disa	able	PPP Authentication PAP or CHAP 💌
ISP Access Setup Username Password Index(1-15) in <u>Sched</u>	Lule Setup:	Idle Timeout -1 second(s) IP Address Assignment Method (IPCP) WAN IP Alias Fixed IP: Yes < No (Dynamic IP)
=>,, ISDN Dial Backup Setu	_,,,	Default MAC Address
Dial Backup Mode	None 💌	Specify a MAC Address
WAN Connection Dete	ction	MAC Address:
Mode	ARP Detect 🛩	
Ping IP	0.0.0	
TTL:	255	

PPPoE Client Mode Click Enable for activating this function. If you click Disable, this function will be closed and all the settings that you adjusted in this page will be invalid. **ISP** Access Setup Enter your allocated username, password and authentication parameters according to the information provided by your ISP. If you want to connect to Internet all the time, you can check Always On. Username – Type in the username provided by ISP in this field. **Password** – Type in the password provided by ISP in this field. Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page. **ISDN Dial Backup** This setting is available for the routers supporting ISDN Setup function only. Before utilizing the ISDN dial backup feature, you must create a dial backup profile first. Please click Internet Access Setup > Dialing to a Single ISP to enter the backup profile. Dial Backup Mode None None Packet Trigger

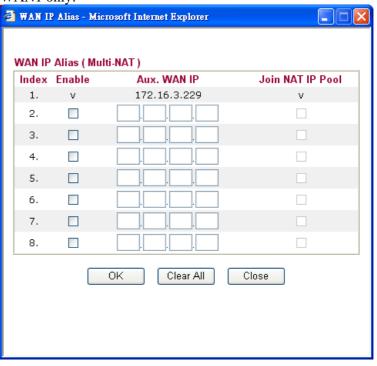
This setting is available for *i* model only.

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

	Packet Trigger - The backup line is not on until a packet from a local host triggers the router to establish a connection.		
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command. 		
PPP/MP Setup	 PPP Authentication – Select PAP only or PAP or CHAP for PPP. Idle Timeout – Set the timeout for breaking down the Internet after passing through the time without any action. This setting is active only when the Active on demand option for Active Mode is selected in WAN>> General Setup page. 		
IP Address Assignment Method (IPCP)	Usually ISP dynamically assigns IP address to you each time you connect to it and request. In some case, your ISP provides service to always assign you the same IP address whenever you request. In this case, you can fill in this IP address in the Fixed IP field. Please contact your ISP before you want to use this function.		

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.



Fixed IP – Click **Yes** to use this function and type in a fixed IP address in the box of **Fixed IP Address**.

Default MAC Address – You can use **Default MAC Address** or specify another MAC address by typing on the boxes of MAC Address for the router.

Specify a MAC Address – Type the MAC address for the router manually.

After finishing all the settings here, please click **OK** to activate them.

Details Page for Static or Dynamic IP

WAN >> Internet Access

For static IP mode, you usually receive a fixed public IP address or a public subnet, namely multiple public IP addresses from your DSL or Cable ISP service providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you could assign an IP address or many IP address to the WAN interface.

To use **Static or Dynamic IP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **Static or Dynamic IP** mode for WAN2. The following web page will be shown.

Static or Dynamic IP (E	HCP Client)	WAN IP Network Settings	WAN IP Alias	
💿 Enable 🔘 Disa	able	Obtain an IP address a	Obtain an IP address automatically	
ISDN Dial Backup Setu	ID	Router Name	*	
Dial Backup Mode	None 💌	Domain Name * : Required for some 1	* ISPs	
Keep WAN Connection	1	Specify an IP address	;	
Enable PING to ke	ep alive	IP Address	172.16.3.229	
PING to the IP		Subnet Mask	255.255.0.0	
PING Interval	0 minute(s)	Gateway IP Address	172.16.3.4	
WAN Connection Dete	ction	 Default MAC Addres 	ss	
Mode	ARP Detect 💌	Specify a MAC Add	ress	
Ping IP	0.0.0.0	MAC Address:		
TTL:	255		5.19	
RIP Protocol		DNS Server IP Address		
Enable RIP		Primary IP Address		
		Secondary IP Address		

Static or Dynamic IP (DHCP Client)	Click Enable for activatin this function will be closed in this page will be invalid	d and all the setting	
ISDN Dial Backup Setup	This setting is available for only. Before utilizing the create a dial backup profil Setup > Dialing to a Sing	ISDN dial backup f e first. Please click	feature, you must Internet Access
	Dial Backup Mode	None None Packet Trigger Always On	

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

	 None - Disable the backup function. Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection. Always On - If the broadband connection is no longer available, the backup line will be activated automatically and always on until the broadband connection is restored. We recommend you to enable this feature if you host a web server for your customers' access.
Keep WAN Connection	 Normally, this function is designed for Dynamic IP environments because some ISPs will drop connections if there is no traffic within certain periods of time. Check Enable PING to keep alive box to activate this function. PING to the IP - If you enable the PING function, please specify the IP address for the system to PING it for keeping alive. PING Interval - Enter the interval for the system to execute the PING operation.
WAN Connection Detection	 Such function allows you to verify whether network connection is alive or not through ARP Detect or Ping Detect. Mode – Choose ARP Detect or Ping Detect for the system to execute for WAN detection. Ping IP – If you choose Ping Detect as detection mode, you have to type IP address in this field for pinging. TTL (Time to Live) – Displays value for your reference. TTL value is set by telnet command.
RIP Protocol	Routing Information Protocol is abbreviated as RIP (RFC1058) specifying how routers exchange routing tables information. Click Enable RIP for activating this function.
WAN IP Network Settings	This group allows you to obtain an IP address automatically and allows you type in IP address manually.
	WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.

1. v 172.16.3.229 v 2. . . . 3. . . . 4. . . . 5. . . . 6. . . .
3. 4. 5. 6.
4.
5.
6.
7.
8.

Obtain an IP address automatically – Click this button to obtain the IP address automatically if you want to use **Dynamic IP** mode. *Router Name:* Type in the router name provided by ISP. *Domain Name:* Type in the domain name that you have assigned. **Specify an IP address** – Click this radio button to specify some data if you want to use **Static IP** mode.

IP Address: Type the IP address.

Subnet Mask: Type the subnet mask.

Gateway IP Address: Type the gateway IP address.

Default MAC Address : Click this radio button to use default MAC address for the router.

Specify a MAC Address: Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

DNS Server IPType in the primary IP address for the router if you want to use**AddressStatic IP** mode. If necessary, type in secondary IP address for
necessity in the future.

Details Page for PPTP/L2TP

To use **PPTP** as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPTP** mode for WAN2. The following web page will be shown.

PPTP/L2TP Client Mode	PPP Setup	PPP Setup	
○Enable PPTP ○Enable L2TP ⊙Disable	PPP Authentication	PAP or CHAP 💙	
Server Address	Idle Timeout	-1 second(s)	
Specify Gateway IP Address	IP Address Assignment M (IPCP) WAN IP Alias		
ISP Access Setup	— Fixed IP: 🔘 Yes 💿 N	No (Dynamic IP)	
Username	Fixed IP Address		
Password	Obtain an IP addres		
Index(1-15) in <u>Schedule</u> Setup:	 Obtain an in address Specify an IP address 	,	
=> , , , , , ,	IP Address		
ISDN Dial Backup Setup	Subnet Mask		
Dial Backup Mode 🛛 None 💌			
Mode establish a tr Enable L21 establish a tr	unnel to a DSL mode (P - Click this radio bunnel to a DSL mode)	outton to enable a PPTP client to em on the WAN interface. button to enable a L2TP client to em on the WAN interface. to close the connection through	
PPTP or L2'	TP.	-	
Server Add	ress - Specify the IP	address of the PPTP/L2TP	

WAN >> Internet Access

Server Address - Specify the IP address of the PPTP/L2TP server if you enable PPTP/L2TP client mode.
 Specify Gateway IP Address – Specify the gateway IP address for DHCP server.
 ISP Access Setup
 Username -Type in the username provided by ISP in this field.
 Password -Type in the password provided by ISP in this field.
 Index (1-15) in Schedule Setup - You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

ISDN Dial BackupThis setting is available for the routers supporting ISDN function
only. Before utilizing the ISDN dial backup feature, you must
create a dial backup profile first. Please click Internet Access
Setup > Dialing to a Single ISP to enter the backup profile.

Dial Backup Mode

	*	None
None		None
Packet Trigger	·	Packet Trigger

Due to the absence of the ISDN interface in some models, the ISDN dial backup feature and its associated setup options are not available to them. Please refer to the previous part for further information.

None - Disable the backup function.

Packet Trigger -The backup line is not on until a packet from a local host triggers the router to establish a connection.

PPP Setup	PPP Authentication - Select PAP only or PAP or CHAP for PPP.
	Idle Timeout - Set the timeout for breaking down the Internet after
	passing through the time without any action. This setting is active
	only when the Active on demand option for Active Mode is
	selected in WAN>> General Setup page.
IP Address	Fixed IP - Usually ISP dynamically assigns IP address to you each
Assignment	time you connect to it and request. In some case, your ISP provides
Method(IPCP)	service to always assign you the same IP address whenever you
	request. In this case, you can fill in this IP address in the Fixed IP
	field. Please contact your ISP before you want to use this function.
	Click Yes to use this function and type in a fixed IP address in the

Fixed IP Address - Type a fixed IP address.

box.

WAN IP Alias - If you have multiple public IP addresses and would like to utilize them on the WAN interface, please use WAN IP Alias. You can set up to 8 public IP addresses other than the current one you are using. Notice that this setting is available for WAN1 only.

🕘 WAN I	P Alias - M	icrosoft Internet Explorer	
WAN IP	PAlias (M	ulti-NAT)	
Index	Enable	Aux. WAN IP	Join NAT IP Pool
1.	v	172.16.3.229	V
2.			
з.			
4.			
5.			
6.			
7.			
8.			
		OK Clear All	Close

Default MAC Address – Click this radio button to use default MAC address for the router.

Specify a MAC Address - Some Cable service providers specify a specific MAC address for access authentication. In such cases you need to click the **Specify a MAC Address** and enter the MAC address in the MAC Address field.

WAN IP Network Settings

Obtain an IP address automatically – Click this button to obtain the IP address automatically.

Specify an IP address – Click this radio button to specify some data.

IP Address – Type the IP address. **Subnet Mask** – Type the subnet mask.

Details Page for PPP

To use **PPP** (for 3G USB Modem) as the accessing protocol of the internet, please choose **Internet Access** from **WAN** menu. Then, select **PPP** mode for WAN2. The following web page will be shown.

WAN >> Internet Access					
WAN 2					
PPP Client Mode	🖲 Enable 🔿 Disable				
SIM PIN code					
Modem Initial String	AT&FE0V1X1&D2&C1S0=0 (Default:AT&FE0V1X1&D2&C1S0=0)				
Modem Dial String	ATDT*99# (Default:ATDT*99#)				
PPP Username	(Optional)				
PPP Password	(Optional)				
Index(1-15) in <u>Schedu</u> =>,,	l <u>e</u> Setup: ,,,				
	OK Cancel Default				
PP Client Mode	Click Enable to activate this mode for WAN2.				
IM PIN code	Type PIN code of the SIM card that will be used to access Interne				
Iodem Initial String	g Such value is used to initialize USB modem. Please use the defaul value. If you have any question, please contact to your ISP.				
Iodem Dial String	Such value is used to dial through USB mode. Please use the default value. If you have any question, please contact to your ISP				
PP Username	Type the PPP username (optional).				
PP Password	Type the PPP password (optional).				
ndex (1-15)	Set the PCs on LAN to work at certain time interval only. You ma choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this filed blank and the function will always work.				

3.1.5 Load-Balance Policy

This router supports the function of load balancing. It can assign traffic with protocol type, IP address for specific host, a subnet of hosts, and port range to be allocated in WAN1 or WAN2 interface. The user can assign traffic category and force it to go to dedicate network interface based on the following web page setup. Twenty policies of load-balance are supported by this router.

Note: Load-Balance Policy is running only when both WAN1 and WAN2 are activated.

WAN >> Load-Balance Policy

Index	Enable	Proto	col	WAN	Src IP Start	Src IP End	Dest IP Start	Dest IP End	Dest Port Start	Dest Port End
1		any	*	WAN1 💌						
<u>2</u>		any	*	WAN1 🔽						
<u>3</u>		any	*	WAN1 💌						
<u>4</u>		any	*	WAN1 🔽						
<u>5</u>		any	*	WAN1 💌						
<u>6</u>		any	*	WAN1 🔽						
Z		any	*	WAN1 💌						
<u>8</u>		any	*	WAN1 🔽						
<u>9</u>		any	*	WAN1 🔽						
<u>10</u>		any	*	WAN1 🔽						
< <u>1-10</u>	11-20 :	•>								<u>Next</u> >

ΟK

Index	Click the number of index to access into the load-balance policy configuration web page.
Enable	Check this box to enable this policy.
Protocol	Use the drop-down menu to change the protocol for the WAN interface.
WAN	Use the drop-down menu to change the WAN interface.
Src IP Start	Displays the IP address for the start of the source IP.
Src IP End	Displays the IP address for the end of the source IP.
Dest IP Start	Displays the IP address for the start of the destination IP.
Dest IP End	Displays the IP address for the end of the destination IP.
Dest Port Start	Displays the IP address for the start of the destination port.
Dest Port End	Displays the IP address for the end of the destination port.

Click Index 1 to access into the following page for configuring load-balance policy.

WAN >> Load-Balance Policy

🗹 Enable	
Protocol	ТСР
Binding WAN interafce	WAN1 💌
Src IP Start	192.168.1.3
Src IP End	192.168.1.5
Dest IP Start	168.95.0.0
Dest IP End	168.95.0.100
Dest Port Start	80
Dest Port End	100

Enable

Check this box to enable this policy.

Protocol

Use the drop-down menu to choose a proper protocol for the WAN interface.

Protocol	

any	*
any	
TCP	
UDP	
TCP/UDP	
ICMP	
IGMP	

Binding WAN interface	Choose the WAN interface (WAN1 or WAN2) for binding.
Src IP Start	Type the source IP start for the specified WAN interface.
Src IP End	Type the source IP end for the specified WAN interface. If this field is blank, it means that all the source IPs inside the LAN will be passed through the WAN interface.
Dest IP Start	Type the destination IP start for the specified WAN interface.
Dest IP End	Type the destination IP end for the specified WAN interface. If this field is blank, it means that all the destination IPs will be passed through the WAN interface.
Dest Port Start	Type the destination port start for the destination IP.
Dest Port End	Type the destination port end for the destination IP. If this field is blank, it means that all the destination ports will be passed through the WAN interface.

3.2 LAN

Local Area Network (LAN) is a group of subnets regulated and ruled by router. The design of network structure is related to what type of public IP addresses coming from your ISP.

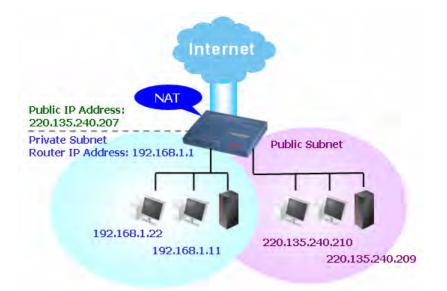


3.2.1 Basics of LAN

The most generic function of Vigor router is NAT. It creates a private subnet of your own. As mentioned previously, the router will talk to other public hosts on the Internet by using public IP address and talking to local hosts by using its private IP address. What NAT does is to translate the packets from public IP address to private IP address to forward the right packets to the right host and vice versa. Besides, Vigor router has a built-in DHCP server that assigns private IP address to each local host. See the following diagram for a briefly understanding.



In some special case, you may have a public IP subnet from your ISP such as 220.135.240.0/24. This means that you can set up a public subnet or call second subnet that each host is equipped with a public IP address. As a part of the public subnet, the Vigor router will serve for IP routing to help hosts in the public subnet to communicate with other public hosts or servers outside. Therefore, the router should be set as the gateway for public hosts.



What is Routing Information Protocol (RIP)

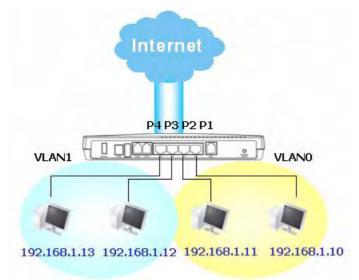
Vigor router will exchange routing information with neighboring routers using the RIP to accomplish IP routing. This allows users to change the information of the router such as IP address and the routers will automatically inform for each other.

What is Static Route

When you have several subnets in your LAN, sometimes a more effective and quicker way for connection is the **Static routes** function rather than other method. You may simply set rules to forward data from one specified subnet to another specified subnet without the presence of RIP.

What are Virtual LANs and Rate Control

You can group local hosts by physical ports and create up to 4 virtual LANs. To manage the communication between different groups, please set up rules in Virtual LAN (VLAN) function and the rate of each.



3.2.2 General Setup

LAN >> General Setup

This page provides you the general settings for LAN.

Click LAN to open the LAN settings page and choose General Setup.

AN IP Network Configurat	tion	DHCP Server Configuration		
For NAT Usage		💿 Enable Server 🔘 Disa	ble Server	
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Su	bnet 🔾 2nd Subnet	
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10	
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50	
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1	
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address		
2n	d Subnet DHCP Server	for Relay Agent DNS Server IP Address		
		Force DNS manual s	setting	
RIP Protocol Control Disable 💌		Primary IP Address		
		Secondary IP Address		

1st IP Address	Type in private IP address for connecting to a local private network (Default: 192.168.1.1).
1st Subnet Mask	Type in an address code that determines the size of the network. (Default: 255.255.255.0/ 24)
For IP Routing Usage	Click Enable to invoke this function. The default setting is Disable .
2 nd IP Address	Type in secondary IP address for connecting to a subnet. (Default: 192.168.2.1/24)
2 nd Subnet Mask	An address code that determines the size of the network. (Default: 255.255.255.0/ 24)
2 nd DHCP Server	You can configure the router to serve as a DHCP server for the 2nd subnet.
	🗿 http://192.168.1.1 - Router Web Configurator - Microsoft Internet Explorer

Start IP Address		
IP Pool Counts	0 (max. 10)	
Index Matched M	AC Address	given IP Address
MAC Address : :	elete Edit	Cancel

Start IP Address: Enter a value of the IP address pool for the
DHCP server to start with when issuing IP addresses. If the 2nd IP
address of your router is 220.135.240.1, the starting IP address
must be 220.135.240.2 or greater, but smaller than
220.135.240.254.

IP Pool Counts: Enter the number of IP addresses in the pool. The maximum is 10. For example, if you type 3 and the 2nd IP address of your router is 220.135.240.1, the range of IP address by the DHCP server will be from 220.135.240.2 to 220.135.240.11.

MAC Address: Enter the MAC Address of the host one by one and click **Add** to create a list of hosts to be assigned, deleted or edited IP address from above pool. Set a list of MAC Address for 2^{nd} DHCP server will help router to assign the correct IP address of the correct subnet to the correct host. So those hosts in 2^{nd} subnet won't get an IP address belonging to 1^{st} subnet.

RIP Protocol Control Disable deactivates the RIP protocol. It will lead to a stoppage of the exchange of routing information between routers. (Default)

RIP Protocol Control Disable

Disable	~
Disable	
1st Subnet	
2nd Subnet	
-	

1st Subnet - Select the router to change the RIP information of the 1st subnet with neighboring routers.

2nd Subnet - Select the router to change the RIP information of the 2nd subnet with neighboring routers.

DHCP ServerDHCP stands for Dynamic Host Configuration Protocol. The
router by factory default acts a DHCP server for your network so it
automatically dispatch related IP settings to any local user
configured as a DHCP client. It is highly recommended that you
leave the router enabled as a DHCP server if you do not have a
DHCP server for your network.

If you want to use another DHCP server in the network other than the Vigor Router's, you can let Relay Agent help you to redirect the DHCP request to the specified location.

Enable Server - Let the router assign IP address to every host in the LAN.

Disable Server – Let you manually assign IP address to every host in the LAN.

Relay Agent – $(1^{st} subnet/2^{nd} subnet)$ Specify which subnet that DHCP server is located the relay agent should redirect the DHCP request to.

Start IP Address - Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses. If the 1st IP address of your router is 192.168.1.1, the starting IP address must be 192.168.1.2 or greater, but smaller than 192.168.1.254.

IP Pool Counts - Enter the maximum number of PCs that you want the DHCP server to assign IP addresses to. The default is 50 and the maximum is 253.

Gateway IP Address - Enter a value of the gateway IP address for the DHCP server. The value is usually as same as the 1st IP address

	DHCP Server the DHCP serve	hich means the router is the IP Address for Relay Agen er you are going to use so th DHCP request to the DHCP	t - Set the IP address of he Relay Agent can help
DNS Server Configuration	have a unique I easy to rememb	Domain Name System. Eve P address, also they may ha ber name such as www.yaho er-friendly name into its equ	ve a human-friendly, bo.com. The DNS server
	in this page inst server (PPPoE, Primary IP Ad here because yo one DNS Serve automatically a to this field. Secondary IP address here be DNS Server. If automatically a 194.98.0.1 to th	anual setting - Force Vigor2 tead of DNS servers given b PPTP, L2TP or DHCP serv dress - You must specify a I our ISP should provide you r. If your ISP does not provid pply default DNS Server IP Address - You can specify s cause your ISP often provid your ISP does not provide i pply default secondary DNS is field. S Server IP address can be	by the Internet Access fer). DNS server IP address with usually more than ide it, the router will address: 194.109.6.66 recondary DNS server IP les you more than one t, the router will S Server IP address:
	LAN Status	Primary DNS: 194.109.6.66	System Optime: 0:7:59 Secondary DNS: 168.95.1.1

TX Packets IP Address 192.168.1.1 490 408 If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a

RX Packets

DNS proxy server and maintain a DNS cache. If the IP address of a domain name is already in the DNS cache, the router will resolve the domain name immediately. Otherwise, the

router forwards the DNS query packet to the external DNS server by establishing a WAN (e.g. DSL/Cable) connection. There are two common scenarios of LAN settings that stated in Chapter 4. For the

configuration examples, please refer to that chapter to get more information for your necessity.

3.2.3 Static Route

Go to LAN to open setting page and choose Static Route.

tatic Route	e Configuration		Set	to Factory Default <u>View R</u>	outing lable
Index	Destination Address	Status	Index	Destination Address	Status
<u>1.</u>	???	?	<u>6.</u>	???	?
<u>2.</u>	???	?	<u>7.</u>	???	?
<u>3.</u>	???	?	<u>8.</u>	???	?
<u>4.</u>	???	?	<u>9.</u>	???	?
<u>5.</u>	???	?	<u>10.</u>	???	?

LAN >> Static Route Setup

Status: v --- Active, x --- Inactive, ? --- Empty

Index	The number (1 to 10) under Index allows you to open next page to set up static route.
Destination Address	Displays the destination address of the static route.
Status	Displays the status of the static route.
Viewing Routing Table	Displays the routing table for your reference.

Diagnostics >> View Routing Table

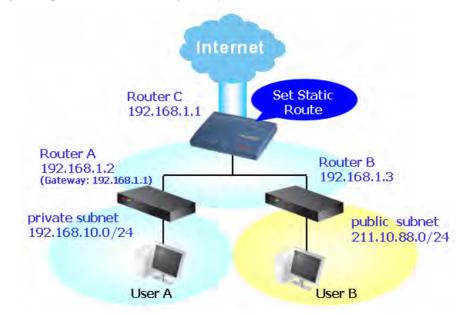
Key: C	- connected, S -	static, R - RIP, * -	default, ~ - priv	ate	
*	0.0.0.0/	0.0.0.0 via 1	72.16.3.1, WAN1		
С~	192.168.1.0/	255.255.255.0 is di	rectly connected,	LAN	
С	172.16.3.0/	255.255.255.0 is di	rectly connected,	WAN1	

Add Static Routes to Private and Public Networks

Here is an example of setting Static Route in Main Router so that user A and B locating in different subnet can talk to each other via the router. Assuming the Internet access has been configured and the router works properly:

- use the Main Router to surf the Internet.
- create a private subnet 192.168.10.0 using an internal Router A (192.168.1.2)
- create a public subnet 211.100.88.0 via an internal Router B (192.168.1.3).
- have set Main Router 192.168.1.1 as the default gateway for the Router A 192.168.1.2.

Before setting Static Route, user A cannot talk to user B for Router A can only forward recognized packets to its default gateway Main Router.



1. Go to LAN page and click General Setup, select 1st Subnet as the RIP Protocol Control. Then click the OK button.

Note: There are two reasons that we have to apply RIP Protocol Control on 1st Subnet. The first is that the LAN interface can exchange RIP packets with the neighboring routers via the 1st subnet (192.168.1.0/24). The second is that those hosts on the internal private subnets (ex. 192.168.10.0/24) can access the Internet via the router, and continuously exchange of IP routing information with different subnets.

2. Click the LAN - Static Route and click on the Index Number 1. Check the Enable box. Please add a static route as shown below, which regulates all packets destined to 192.168.10.0 will be forwarded to 192.168.1.2. Click OK.

ndex No. 1		
🗹 Enable		
	Destination IP Address	192.168.10.0
	Subnet Mask	255.255.255.0
	Gateway IP Address	192.168.1.2
	Network Interface	LAN 🛩

3. Return to **Static Route Setup** page. Click on another **Index Number** to add another static route as show below, which regulates all packets destined to 211.100.88.0 will be forwarded to 192.168.1.3.

stination IP Address	211.100.88.0	
ibnet Mask	255.255.255.0	
iteway IP Address	192.168.1.3	
twork Interface	LAN 🛩	
	stination IP Address Ibnet Mask Iteway IP Address Itwork Interface	abnet Mask 255.255.250 ateway IP Address 192.168.1.3

4. Go to **Diagnostics** and choose **Routing Table** to verify current routing table.

Diagnostics >> View Routing Table

Key: C	C - connected, S -	static, R - RIP, * - default, ~ - private	
s~	192.168.10.0/	255.255.255.0 via 192.168.1.2, IFO	
С~	192.168.1.0/	255.255.255.0 is directly connected, IFO	
S~	211.100.88.0/	255.255.255.0 via 192.168.1.3, IFO	

3.2.4 Bind IP to MAC

This function is used to bind the IP and MAC address in LAN to have a strengthen control in network. When this function is enabled, all the assigned IP and MAC address binding together cannot be changed. If you modified the binding IP or MAC address, it might cause you not access into the Internet.

Click LAN and click Bind IP to MAC to open the setup page.

LAN >> Bind IP to MAC

Bind IP to MAC		
Note: IP-MAC binding presets DHCP Allo	cations.	
If you select Strict Bind, unspecif	ied LAN clients cannot access t	he Internet.
💿 Enable 🔿 Disable 🔿 Strict Bind		
ARP Table Select All Sort Refre	esh IP Bind List	<u>Select All</u> Sort
IP Address Mac Address 192.168.1.13 00-0E-A6-2A-D5-A1 192.168.1.10 00-0D-0B-A7-86-F3 192.168.1.100 00-08-A1-36-97-5D		Mac Address
Add and Edit		
IP Address		
Mac Address :::::::::::::::::::::::::::::::::::		
A	sdd Edit Delete	

Enable	Click this radio button to invoke this function. However, IP/MAC which is not listed in IP Bind List also can connect to Internet.
Disable	Click this radio button to disable this function. All the settings on this page will be invalid.
Strict Bind	Click this radio button to block the connection of the IP/MAC which is not listed in IP Bind List.
ARP Table	This table is the LAN ARP table of this router. The information for IP and MAC will be displayed in this field. Each pair of IP and MAC address listed in ARP table can be selected and added to IP Bind List by clicking Add below.
Add and Edit	 IP Address - Type the IP address that will be used for the specified MAC address. Mac Address - Type the MAC address that is used to bind with the assigned IP address.
Refresh	It is used to refresh the ARP table. When there is one new PC added to the LAN, you can click this link to obtain the newly ARP table information.
IP Bind List	It displays a list for the IP bind to MAC information.

Add	It allows you to add the one you choose from the ARP table or the IP/MAC address typed in Add and Edit to the table of IP Bind List .
Edit	It allows you to edit and modify the selected IP address and MAC address that you create before.
Delete	You can remove any item listed in IP Bind List . Simply click and select the one, and click Delete . The selected item will be removed from the IP Bind List .
•	u select Strict Bind , you have to bind one set of IP/MAC address for one the of the PCs can access into Internet. And the web configurator of the be accessed.

3.3 NAT

Usually, the router serves as an NAT (Network Address Translation) router. NAT is a mechanism that one or more private IP addresses can be mapped into a single public one. Public IP address is usually assigned by your ISP, for which you may get charged. Private IP addresses are recognized only among internal hosts.

When the outgoing packets destined to some public server on the Internet reach the NAT router, the router will change its source address into the public IP address of the router, select the available public port, and then forward it. At the same time, the router shall list an entry in a table to memorize this address/port-mapping relationship. When the public server response, the incoming traffic, of course, is destined to the router's public IP address and the router will do the inversion based on its table. Therefore, the internal host can communicate with external host smoothly.

The benefit of the NAT includes:

- Save cost on applying public IP address and apply efficient usage of IP address. NAT allows the internal IP addresses of local hosts to be translated into one public IP address, thus you can have only one IP address on behalf of the entire internal hosts.
- Enhance security of the internal network by obscuring the IP address. There are many attacks aiming victims based on the IP address. Since the attacker cannot be aware of any private IP addresses, the NAT function can protect the internal network.

On NAT page, you will see the private IP address defined in RFC-1918. Usually we use the 192.168.1.0/24 subnet for the router. As stated before, the NAT facility can map one or more IP addresses and/or service ports into different specified services. In other words, the NAT function can be achieved by using port mapping methods.

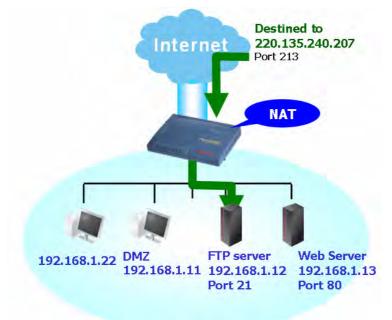
Below shows the menu items for NAT.



3.3.1 Port Redirection

Port Redirection is usually set up for server related service inside the local network (LAN), such as web servers, FTP servers, E-mail servers etc. Most of the case, you need a public IP address for each server and this public IP address/domain name are recognized by all users.

Since the server is actually located inside the LAN, the network well protected by NAT of the router, and identified by its private IP address/port, the goal of Port Redirection function is to forward all access request with public IP address from external users to the mapping private IP address/port of the server.



The port redirection can only apply to incoming traffic.

To use this function, please go to **NAT** page and choose **Port Redirection** web page. The **Port Redirection Table** provides 10 port-mapping entries for the internal hosts.

#	Mode	Service Name	Protocol	Public Port	Private IP	Private Port	Active
1	Range 💌		💙	0 -		0	
2	Single 🔽		💙	0		0	
3	Single 🔽		💙	0		0	
4	Single 🔽		🗸	0		0	
5	Single 🔽		🗸	0		0	
6	Single 🔽		🖌	0		0	
7	Single 💌		🖌	0		0	
8	Single 💌		🖌	0		0	
9	Single 💌		🖌	0		0	
10	Single 🔽		🗸	0		0	

NAT >> Configure Port Redirection Table

Note: In "Range" Mode the End Port will be calculated automatically once the Start IP, End IP and Private Port have been entered.

	OK Cancel
Mode	Two options are provided here for you to choose. To set a range for the specific service, select Range.
Service Name	Enter the description of the specific network service.
Protocol	Select the transport layer protocol (TCP or UDP).

Public Port	Specify which port can be redirected to the specified Private IP and Port of the internal host. If you choose Range as the port redirection mode, you will see two boxes on this field. Simply type the required number on the first box. The second one will be assigned automatically later.			
Private IP	Specify the private IP address of the internal host providing the service. If you choose Range as the port redirection mode, you will see two boxes on this field. Type a complete IP address in the first box (as the starting point) and the fourth digits in the second box (as the end point).			
Private Port	Specify the private port number of the service offered by the internal host.			
Active	Check this box to activate the port-mapping entry you have defined.			

Note that the router has its own built-in services (servers) such as Telnet, HTTP and FTP etc. Since the common port numbers of these services (servers) are all the same, you may need to reset the router in order to avoid confliction.

For example, the built-in web configurator in the router is with default port 80, which may conflict with the web server in the local network, http://192.168.1.13:80. Therefore, you need to **change the router's http port to any one other than the default port 80** to avoid conflict, such as 8080. This can be set in the **System Maintenance** >>**Management Setup**. You then will access the admin screen of by suffixing the IP address with 8080, e.g., http://192.168.1.1:8080 instead of port 80.

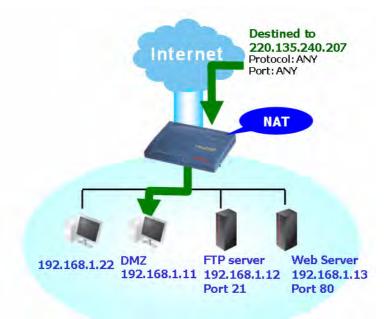
System Maintenance >> Management

Management Access Control	Management Port Setup	
	💿 User Define Ports	🔘 Default Ports
Allow management from the Internet	Telnet Port	23 (Default: 23)
HTTP Server	HTTP Port	80 (Default: 80) 443 (Default: 443)
HTTPS Server Telnet Server	FTP Port	21 (Default: 21)
SSH Server	SSH Port	22 (Default: 22)
Disable PING from the Internet	SNMP Setup	
Access List	🔲 Enable SNMP Agent	:
List IP Subnet Mask	Get Community	public
	Set Community	private
2 2 2	Manager Host IP	
	Trap Community	public
	Notification Host IP	
	Trap Timeout	10 seconds

3.3.2 DMZ Host

As mentioned above, **Port Redirection** can redirect incoming TCP/UDP or other traffic on particular ports to the specific private IP address/port of host in the LAN. However, other IP protocols, for example Protocols 50 (ESP) and 51 (AH), do not travel on a fixed port. Vigor router provides a facility **DMZ Host** that maps ALL unsolicited data on any protocol to a single host in the LAN. Regular web surfing and other such Internet activities from other

clients will continue to work without inappropriate interruption. **DMZ Host** allows a defined internal user to be totally exposed to the Internet, which usually helps some special applications such as Netmeeting or Internet Games etc.



The inherent security properties of NAT are somewhat bypassed if you set up DMZ host. We suggest you to add additional filter rules or a secondary firewall.

Click **DMZ Host** to open the following page:

NAT >> DMZ Host Setup

DMZ Host Setup	
WAN 1	
Active True IP 🔽	
Private IP	Choose PC
MAC Address of the T	rue IP DMZ Host 00 , 00 , 00 , 00 , 00 , 00 , 00
Note : When a True-I always on.	P DMZ host is turned on, it will force the router's WAN connection to be
WAN 2	
Enable	Private IP
\checkmark	Choose PC
WAN1	This page allows you to set Private IP or Active True IP as the DMZ host.
	Active True IP V None Private IP Active True IP
Private IP	If you choose Private IP as the selection for DMZ host, pleas type in private IP or select any one by clicking the Choose P button.

MAC Address of the TrueIf you choose Active True IP as the selection for DMZ host,IP DMZ Hostplease type in MAC address in these fields.

If you previously have set up WAN IP Alias on WAN1 interface while configuring PPPoE, Static or Dynamic IP or PPTP (by accessing into WAN>>Internet Access), you will find them in Aux. WAN IP list for your selection.

DMZ Host Setup WAN 1 Index Enable 2. WAN 2 Enable Private IP Choose PC	172.16.3.229 172.16.3.89 Check the Enter the to select Click the depicte address address address	OK to enable th ne private I t one. nis button a d below. T es of all ho	IP address of and then a w he window	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	Choose PC Choose PC Choose PC Choose PC
Index Enable 1. 2. UNAN 2 Enable Enable Private IP	172.16.3.229 172.16.3.89 Check the Enter the to select Click the depicte address address address	OK to enable the private I t one. his button a d below. The es of all ho in the list	Private IP Clear the DMZ Ho IP address of and then a w be window osts in your	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	Choose PC Choose PC , or click Choose PC omatically pop up, a t of private IP
1. 2. WAN 2 Enable Enable Private IP	172.16.3.229 172.16.3.89 Check the Enter the to select Click the depicte address address address	OK to enable the private I t one. his button a d below. The es of all ho in the list	Private IP Clear the DMZ Ho IP address of and then a w be window osts in your	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	Choose PC Choose PC , or click Choose PC omatically pop up, a t of private IP
2. WAN 2 Enable Private IP	172.16.3.89 Check the Enter the to select Click the depicteen addressen addr	OK to enable the private I t one. his button a d below. The es of all ho in the list	Clear the DMZ Ho P address of and then a v the window osts in your	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	Choose PC Choose PC , or click Choose PC omatically pop up, a t of private IP
WAN 2 Enable Private IP	Check the Enter the to select Click the depicte address address address	to enable the private I t one. his button a d below. T es of all ho in the list	Clear the DMZ Ho P address of and then a v the window osts in your	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	Choose PC , or click Choose PC omatically pop up, a t of private IP
Enable Private IP	Check the Enter the to select Click the depicte address address address	to enable the private I t one. his button a d below. T es of all ho in the list	Clear the DMZ Ho P address of and then a v the window osts in your	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	, or click Choose PC omatically pop up, a t of private IP
Enable Private IP	Check the Enter the to select Click the depicte address address address	to enable the private I t one. his button a d below. T es of all ho in the list	Clear the DMZ Ho P address of and then a v the window osts in your	ost function. of the DMZ host, window will auto v consists of a list r LAN network. S	, or click Choose PC omatically pop up, a t of private IP
Enable Private IP	Enter th to select Click th depicte address address Address	to enable the private I t one. his button a d below. T es of all ho in the list	he DMZ Ho IP address of and then a w he window osts in your	of the DMZ host, window will auto consists of a list r LAN network. S	, or click Choose PC omatically pop up, a t of private IP
Private IP	Enter th to select Click th depicte address address Address	to enable the private I t one. his button a d below. T es of all ho in the list	he DMZ Ho IP address of and then a w he window osts in your	of the DMZ host, window will auto consists of a list r LAN network. S	omatically pop up, a t of private IP
Private IP	Enter th to select Click th depicte address address Address	ne private I at one. his button a d below. T es of all ho in the list	IP address of and then a v 'he window osts in your	of the DMZ host, window will auto consists of a list r LAN network. S	omatically pop up, a t of private IP
	to select Click th depicte address address Address	t one. his button a d below. T es of all ho in the list	and then a v he window osts in your	window will auto consists of a list r LAN network. S	omatically pop up, a t of private IP
Choose PC	depicte address address address	d below. These of all he list	he window osts in your	v consists of a list r LAN network. S	t of private IP
	When y	2.168.1.18 700 have se			the above dialog, th reen. Click OK to
		e setting.	5110 WH OH	the following set	
	NAT >> DM2				
	DMZ Host S	etun			
	WAN 1	smb			
	Index		IX. WAN IP	Private IP	(0k D0)
	1.		2.16.3.229	192.168.1.10	Choose PC
	2.		2.16.3.89		Choose PC

Enable

OK Clear

ſ

Private IP

3.3.3 Open Ports

Open Ports allows you to open a range of ports for the traffic of special applications. Common application of Open Ports includes P2P application (e.g., BT, KaZaA, Gnutella, WinMX, eMule and others), Internet Camera etc. Ensure that you keep the application involved up-to-date to avoid falling victim to any security exploits.

Click **Open Ports** to open the following page:

NAT >> Open Ports

Index	Comment	WAN Interface	Local IP Address	Status
<u>1.</u>				×
<u>2.</u>				×
<u>3.</u>				×
<u>4.</u>				×
<u>5.</u>				×
<u>6.</u>				×
<u>7.</u>				×
<u>8.</u>				×
<u>9.</u>				×
<u>10.</u>				×

Index	Indicate the relative number for the particular entry that you want to offer service in a local host. You should click the appropriate index number to edit or clear the corresponding entry.	
Comment	Specify the name for the defined network service.	
WAN Interface	Display the WAN interface for the entry.	
Local IP Address	Display the private IP address of the local host offering the service.	
Status	Display the state for the corresponding entry. X or V is to represent the Inactive or Active state.	

To add or edit port settings, click one index number on the page. The index entry setup page will pop up. In each index entry, you can specify **10** port ranges for diverse services.

NAT >> Open Ports >> Edit Open Ports

✓ E	Enable Open P	orts						
Comment		P2P	P2P					
WAN Interface			WA	N1 🔽				
WAN IP			172	172.16.3.229 🗸				
	Lo	cal Computer	192.	168.1.10	Cho	ose PC		
	Protocol	Start Port	End Port		Protocol	Start Port	End Port	
1.	TCP 🔽	4500	4700	6.	💌	0	0	
2.	UDP 🔽	4500	4700	7.	💙	0	0	
з.	💙	0	0	8.	💙	0	0	
4.	💙	0	0	9.	💙	0	0	
5.	🗸	0	0	10.	💙	0	0	

Enable Open Ports	Check to enable this entry.
Comment	Make a name for the defined network application/service.
WAN Interface	Specify the WAN interface that will be used for this entry.
WAN IP	Choose one of the WAN IPs from this drop-down list. This selection is available and can be seen only if you have set WAN IP Alias previously.
Local Computer	Enter the private IP address of the local host or click Choose PC to select one.
Choose PC	Click this button and, subsequently, a window having a list of private IP addresses of local hosts will automatically pop up. Select the appropriate IP address of the local host in the list.
Protocol	Specify the transport layer protocol. It could be TCP , UDP , or (none) for selection.
Start Port	Specify the starting port number of the service offered by the local host.
End Port	Specify the ending port number of the service offered by the local host.

3.4 Objects and Groups

For IPs in a range and service ports in a limited range usually will be applied in configuring router's settings, therefore we can define them with *objects* and bind them with *groups* for using conveniently. Later, we can select that object/group that can apply it. For example, all the IPs in the same department can be defined with an IP object (a range of IP address).

Objects and Groups
IP Object
IP Group
Service Type Object
Service Type Group
CSM Profile

Objects Setting >> IP Object

Objects Setting >> IP Object

3.4.1 IP Object

You can set up to 192 sets of IP Objects with different conditions.

Object Profiles:		Set to Factory Defau	
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

Click the number under Index column for settings in detail.

Name:	RD Department
Interface:	Any 💌
Address Type:	Range Address 🐱
Start IP Address:	192.168.1.64
End IP Address:	192.168.1.75
Subnet Mask:	0.0.0.0
Invert Selection:	

Name

Type a name for this profile. Maximum 15 characters are allowed.

Interface	Choose a proper interface (WAN, LAN or Any).		
	Interface: Any Any LAN WAN For example, the Direction setting in Edit Filter Rule will ask you specify IP or IP range for WAN or LAN or any IP address. If you choose LAN as the Interface here, and choose LAN as the direction setting in Edit Filter Rule , then all the IP addresses specified with LAN interface will be opened for		
	you to choose in Edit Filter Rule page.		
Address Type	 Determine the address type for the IP address. Select Single Address if this object contains one IP address only. Select Range Address if this object contains several IPs within a range. Select Subnet Address if this object contains one subnet for IP address. Select Any Address if this object contains any IP address. 		
Start IP Address	Type the start IP address for Single Address type.		
End IP Address	Type the end IP address if the Range Address type is selected.		
Subnet Mask	Type the subnet mask if the Subnet Address type is selected.		
Invert Select	If it is checked, all the IP addresses except the ones listed above will be applied later while it is chosen.		

Below is an example of IP objects settings.

Objects Setting >> IP Object	

Object Profiles:			
Index	Name	Index	
<u>1.</u>	RD Department	<u>17.</u>	
<u>2.</u>	Financial Dept.	<u>18.</u>	
<u>3.</u>	HR Department	<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	

3.4.2 IP Group

This page allows you to bind several IP objects into one IP group.

```
Objects Setting >> IP Group
```

IP Group Table:			Set to Factory Default
Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

```
Objects Setting >> IP Group
```

Name:	Administration
Interface:	Any 🗸
Available IP Objects	Selected IP Objects
1-RD Department 2-Financial Dept. 3-HR Department	* *
	OK Cancel
Name	Type a name for this profile. Maximum 15 characters are allowed.
Interface	Choose WAN, LAN or Any to display all the available IP objects with the specified interface.
Available IP Objects	All the available IP objects with the specified interface chosen above will be shown in this box.
Selected IP Objects	Click >> button to add the selected IP objects in this box.

3.4.3 Service Type Object

Objects Setting >> Service Type Object

You can set up to 96 sets of Service Type Objects with different conditions.

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

```
Objects Setting >> Service Type Object Setup
 Profile Index : 1
                                          www
             Name
                                          TCP
             Protocol
                                                  v
                                           = 🗸
                                                        ~ 65535
             Source Port
                                                1
                                          = 🗸
                                                80
                                                        ~ 80
             Destination Port
                                   ΟK
                                            Cancel
Name
                                Type a name for this profile.
Protocol
                                Specify the protocol(s) which this profile will apply to.
                                 TCP
                                Any
                                ICMP
                                IGMP
                                TCP.
                                UDP
                                 TCP/UDP
                                 Other
Source/Destination Port
                                Source Port and the Destination Port column are available
                                for TCP/UDP protocol. It can be ignored for other protocols.
                                The filter rule will filter out any port number.
                                (=) – when the first and last value are the same, it indicates
                                one port; when the first and last values are different, it
                                indicates a range for the port and available for this profile.
```

(!=) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.(<) – the port number less than this value is available for this profile.

Below is an example of service type objects settings.

Service Type Object Profiles:

Index	Name
<u>1.</u>	SIP
<u>2.</u>	RTP
<u>3.</u>	
1	

3.4.4 Service Type Group

Objects Setting >> Service Type Group

This page allows you to bind several service types into one group.

Group	Name	Group	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

Profile Index : 1 Name:	VolP
Available Service Type Obj	iects Selected Service Type Objects
1-SIP 2-RTP	» «
	OK Cancel
Name	Type a name for this profile.
Available Service Type Objects	You can add IP objects from IP Objects page. All the available IP objects will be shown in this box.
Selected Service Type Objects	Click >> button to add the selected IP objects in this box

3.4.5 CSM Profile

Objects Setting >> CSM Profile

You can define policy profiles for different policy of IM (Instant Messenger)/P2P (Peer to Peer) application. CSM profile will be applied by **Firewall**.

SM Profile Table:			Set to Factory Defaul
Profile	Name	Profile	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

Set to Factory Default Clear all profiles.

Ob	jects	Setting	>>	CSM	Profile
----	-------	---------	----	-----	---------

file Name: CSM-1				
eck for Disallow :				
IM		VoIP		
MSN Ya	hoo Messenger 🛛 ICQ			
AIM QQ	iChat			
Google Talk		jajah		
🔲 Web IM (http://ww	w.e-messenger.net/)	Skype		
Web MSN (http://w	ebmessenger.msn.com/)			
		1		
	P2P			
Protocol	i i i i i i i i i i i i i i i i i i i	Applications		
SoulSeek SoulSeek				
eDonkey eDonkey, eMule, Sł		ireaza		
🗌 FastTrack KazaA, iMesh				
🔲 Gnutella	BearShare, Limewire, Shar	eaza		
BitTorrent	BitTorrent			
	OK Cancel			
ofile Name	Type a name for	the CSM profile. The profile name w		
	•	ontent Security Management drop do		

There are several items for IM, VoIP, P2P provided here for you to choose to disallow people using. Simple check the box (es) and then click **OK**. Later, in the **Firewall>>General Setup** and **Firewall>>Edit Filter Set>>Edit Filter Rule** pages, you can use **Content Security Management** drop down list to choose a proper CSM profile as the standard for all the host(s) or specified host(s) to follow.

in the pages of **Firewall>>General Setup** and **Firewall>>Edit Filter Set>>Edit Filter Rule.**

3.5 Firewall

3.5.1 Basics for Firewall

While the broadband users demand more bandwidth for multimedia, interactive applications, or distance learning, security has been always the most concerned. The firewall of the Vigor router helps to protect your local network against attack from unauthorized outsiders. It also restricts users in the local network from accessing the Internet. Furthermore, it can filter out specific packets that trigger the router to build an unwanted outgoing connection.

The most basic security concept is to set user name and password while you install your router. The administrator login will prevent unauthorized access to the router configuration from your router.

Quick Start Wizard

Please enter an alpha-num	ric string as your Password (Max 23 characters).	
New Password	••••	
Confirm Password	••••	

If you did not set password during installation; you can go to **System Maintenance** to set up your password.

nistrator Password			
Old I	Password		
New	Password		
Conf	firm Password		

Firewall Facilities

System Maintenance >> Administrator Password Setup

The users on the LAN are provided with secured protection by the following firewall facilities:

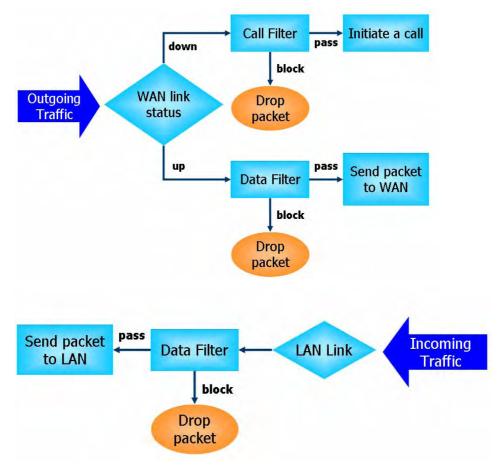
- User-configurable IP filter (Call Filter/ Data Filter).
- Stateful Packet Inspection (SPI): tracks packets and denies unsolicited incoming data
- Selectable Denial of Service (DoS) /Distributed DoS (DDoS) attacks protection
- URL Content Filter

IP Filters

Depending on whether there is an existing Internet connection, or in other words "the WAN link status is up or down", the IP filter architecture categorizes traffic into two: **Call Filter** and **Data Filter**.

- **Call Filter** When there is no existing Internet connection, **Call Filter** is applied to all traffic, all of which should be outgoing. It will check packets according to the filter rules. If legal, the packet will pass. Then the router shall **"initiate a call"** to build the Internet connection and send the packet to Internet.
- **Data Filter** When there is an existing Internet connection, **Data Filter** is applied to incoming and outgoing traffic. It will check packets according to the filter rules. If legal, the packet will pass the router.

The following illustrations are flow charts explaining how router will treat incoming traffic and outgoing traffic respectively.



Stateful Packet Inspection (SPI)

Stateful inspection is a firewall architecture that works at the network layer. Unlike legacy static packet filtering, which examines a packet based on the information in its header, stateful inspection builds up a state machine to track each connection traversing all interfaces of the firewall and makes sure they are valid. The stateful firewall of Vigor router not just examine the header information also monitor the state of the connection.

Content Security Management (CSM)

As the popularity of all kinds of instant messenger application arises, communication cannot become much easier. Nevertheless, while some industry may leverage this as a great tool to connect with their customers, some industry may take reserve attitude in order to reduce employee misusage during office hour or prevent unknown security leak. It is similar situation for corporation towards peer-to-peer applications since file-sharing can be convenient but insecure at the same time. To address these needs, we provide CSM functionality.

Denial of Service (DoS) Defense

The **DoS Defense** functionality helps you to detect and mitigate the DoS attack. The attacks are usually categorized into two types, the flooding-type attacks and the vulnerability attacks. The flooding-type attacks will attempt to exhaust all your system's resource while the vulnerability attacks will try to paralyze the system by offending the vulnerabilities of the protocol or operation system.

The **DoS Defense** function enables the Vigor router to inspect every incoming packet based on the attack signature database. Any malicious packet that might duplicate itself to paralyze the host in the secure LAN will be strictly blocked and a Syslog message will be sent as warning, if you set up Syslog server.

Also the Vigor router monitors the traffic. Any abnormal traffic flow violating the pre-defined parameter, such as the number of thresholds, is identified as an attack and the Vigor router will activate its defense mechanism to mitigate in a real-time manner.

The below shows the attack types that DoS/DDoS defense function can detect:

- 1. SYN flood attack
- 2. UDP flood attack
- 3. ICMP flood attack
- 4. TCP Flag scan
- 5. Trace route
- 6. IP options
- 7. Unknown protocol
- 8. Land attack

9. Smurf attack
10. SYN fragment
11. ICMP fragment
12. Tear drop attack
13. Fraggle attack
14. Ping of Death attack
15. TCP/UDP port scan

Content Filtering

To provide an appropriate cyberspace to users, Vigor router equips with **URL Content Filter** not only to limit illegal traffic from/to the inappropriate web sites but also prohibit other web feature where malicious code may conceal.

Once a user type in or click on an URL with objectionable keywords, URL keyword blocking facility will decline the HTTP request to that web page thus can limit user's access to the website. You may imagine **URL Content Filter** as a well-trained convenience-store clerk who won't sell adult magazines to teenagers. At office, **URL Content Filter** can also provide a job-related only environment hence to increase the employee work efficiency. How can URL Content Filter work better than traditional firewall in the field of filtering? Because it checks the URL strings or some of HTTP data hiding in the payload of TCP packets while legacy firewall inspects packets based on the fields of TCP/IP headers only.

On the other hand, Vigor router can prevent user from accidentally downloading malicious codes from web pages. It's very common that malicious codes conceal in the executable objects, such as ActiveX, Java Applet, compressed files, and other executable files. Once downloading these types of files from websites, you may risk bringing threat to your system. For example, an ActiveX control object is usually used for providing interactive web feature. If malicious code hides inside, it may occupy user's system.

Web Filtering

We all know that the content on the Internet just like other types of media may be inappropriate sometimes. As a responsible parent or employer, you should protect those in your trust against the hazards. With Web filtering service of the Vigor router, you can protect your business from common primary threats, such as productivity, legal liability, network and security threats. For parents, you can protect your children from viewing adult websites or chat rooms.

Once you have activated your Web Filtering service in Vigor router and chosen the categories of website you wish to restrict, each URL address requested (e.g.www.bbc.co.uk) will be checked against our server database, powered by SurfControl. The database covering over 70 languages and 200 countries, over 1 billion Web pages divided into 40 easy-to-understand categories. This database is updated as frequent as daily by a global team of Internet researchers. The server will look up the URL and return a category to your router. Your Vigor router will then decide whether to allow access to this site according to the categories you have selected. Please note that this action will not introduce any delay in your Web surfing because each of multiple load balanced database servers can handle millions of requests for categorization.

Below shows the menu items for Firewall.

Firewall
General Setup
Filter Setup
DoS Defense
URL Content Filter
Web Content Filter

3.5.2 General Setup

Firewall >> General Setup

General Setup allows you to adjust settings of IP Filter and common options. Here you can enable or disable the **Call Filter** or **Data Filter**. Under some circumstance, your filter set can be linked to work in a serial manner. So here you assign the **Start Filter Set** only. Also you can configure the **Log Flag** settings, **Apply IP filter to VPN incoming packets**, and **Accept incoming fragmented UDP packets**.

Click Firewall and click General Setup to open the general setup page.

Call Filter	💽 Enable	Start Filter	Set Set#1 💙
	🔘 Disable		
Data Filter	💿 Enable	Start Filter	Set Set#2 💙
	🔘 Disable		
Actions for defau	lt rule:		
Application		Action/Profile	Log
Filter		Pass 🚩	
Content Security	<u>Management</u>	None 🚩	
🗌 Apply IP filte	r to VPN incoming	packets	
,	5	•	ets (for some games, ex. CS)
	niconning nagmon	tod obi of tohin paol	

Call Filter	Check Enable to activate the Call Filter function. Assign a start filter set for the Call Filter.			
Data Filter	Check Enable to activate the Data Filter filter set for the Data Filter.	function. Assign a start		
Filter	Default rule is applied in this page. Pass – All the packets are allowed to pass through the router without considering settings configured in Firewall>>Filter Block - All the packets are not allowed to pass through the ro without considering settings configured in Firewall>>Filter			
	Filter	Pass 💙 Pass Block		
	For troubleshooting needs, you can spec information by checking the Log box. It server. Please refer to section 3.14.4 Sys detailed information.	will be sent to Syslog		
Content Security Management	Select one of the CSM profiles (configu Groups>>CSM Profiles) for global IM blocking. All the hosts in LAN must foll configured in the CSM profile selected I	/P2P application low the standard		
	For troubleshooting needs, you can specify to record CSM information by checking the Log box. It will be sent to Syslog server. Please refer to section 3.14.4 Syslog/Mail Alert for more detailed information.			
Some on line games (for	example: Half Life) will use lots of frage	nented UDP packets to		

Some on-line games (for example: Half Life) will use lots of fragmented UDP packets to transfer game data. Instinctively as a secure firewall, Vigor router will reject these fragmented packets to prevent attack unless you enable "Accept large incoming fragmented UDP or ICMP Packets". By checking this box, you can play these kinds of on-line games. If security concern is in higher priority, you cannot enable "Accept large incoming fragmented UDP or ICMP Packets".

3.5.3 Filter Setup

Firewall >> Filter Setup

Click **Firewall** and click **Filter Setup** to open the setup page.

Filter Se	tup		Set to Factory Default
Set	Comments	Set	Comments
<u>1.</u>	Default Call Filter	<u>7.</u>	
<u>2.</u>	Default Data Filter	<u>8.</u>	
<u>3.</u>		<u>9.</u>	
<u>4.</u>		<u>10.</u>	
<u>5.</u>		<u>11.</u>	
<u>6.</u>		<u>12.</u>	

To edit or add a filter, click on the set number to edit the individual set. The following page will be shown. Each filter set contains up to 7 rules. Click on the rule number button to edit each rule. Check **Active** to enable the rule.

Firewall >> F	ilter Setup >> Edit F	ilter Set		
Filter Set 1 Comments :	Default Call Filter			
Filter Rul		Comments	Move Up	Move Down
1		Block NetBios		<u>Down</u>
2			<u>UP</u>	Down
3			<u>UP</u>	Down
4			<u>UP</u>	<u>Down</u>
5			<u>UP</u>	<u>Down</u>
6			<u>UP</u>	<u>Down</u>
7			<u>UP</u>	
			Next Filte	er Set None 👻
		OK Clear Canc	el	
lter Ru	le	Click a button numbered button will open Edit Filt information, refer to the f	er Rule web pag	
ctive		Enable or disable the filte	er rule.	
ommen	t	Enter filter set comments	description. Ma	aximum leng

mmentEnter filter set comments/description. Maximum length is
23-character long.

Move Up/Down Use Up or Down link to move the order of the filter rules.

Next Filter SetSet the link to the next filter set to be executed after the current
filter run. Do not make a loop with many filter sets.

To edit Filter Rule, click the Filter Rule index button to enter the Filter Rule setup page.

Firewall >> Edit Filter Set >> Edit Filter Rule

🗹 Check to enable the Filter Rule	3	
Comments:	Block NetBios	
Index(1-15) in <u>Schedule</u> Setup:	,,,,	
Direction:	LAN -> WAN 💌	
Source IP:	Any	Edit
Destination IP:	Any	Edit
Service Type:	TCP/UDP, Port: from 137~139 to any	Edit
Fragments:	Don't Care 💌	
Application	Action/Profile	Syslog
Filter:	Block Immediately	
Branch to Other Filter Set:	None 🔽	
Content Security Management:	None 🗸	

OK	Clear	Cancel
----	-------	--------

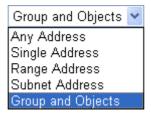
Check to enable the Filter Rule	Check this box to enable the filter rule.
Comments	Enter filter set comments/description. Maximum length is 14- character long.
Index (1-15)	Set the PCs on LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in

Applications >> Schedule setup. The default setting of this filed is blank and the function will always work.

- Direction Set the direction of packet flow (LAN->WAN/WAN->LAN). It is for Data Filter only. For the Call Filter, this setting is not available since Call Filter is only applied to outgoing traffic.
- Source/Destination IP Click Edit to access into the following dialog to choose the source/destination IP or IP ranges.

🕘 IP Address	Edit - Microsoft Internet Explorer		
IP A	ddress Edit		
	Address Type	Group and Objects 💙	
	Start IP Address	0.0.0.0	
	End IP Address	0.0.0.0	
	Subnet Mask	0.0.0.0	
	Invert Selection		
	<u>IP Group</u>	None 💌	
	or <u>IP Object</u>	None 🖌	
	or IP Object	None 1-RD Department	
	or IP Object	2-Financial Dept.	
		3-HR Department	
	OK	Close	

To set the IP address manually, please choose Any Address/Single Address/Range Address/Subnet Address as the Address Type and type them in this dialog. In addition, if you want to use the IP range from defined groups or objects, please choose Group and **Objects** as the Address Type.



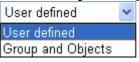
From the **IP Group** drop down list, choose the one that you want to apply. Or use the IP Object drop down list to choose the object that you want.

Click Edit to access into the following dialog to choose a suitable service type.

Service Type

Service Type	Group and Objects 🍟
Protocol	TCP/UDP
Source Port	= 🔽 137 ~ 139
Destination Port	= 🔽 1 ~65535
Service Group	None 🛩
or <u>Service Object</u>	None 💙
or Service Object	None 1-SIP
or Service Object	2-RTP
	OK Close

the Service Type and type them in this dialog. In addition, if you want to use the service type from defined groups or objects, please choose **Group and Objects** as the Service Type.



Protocol - Specify the protocol(s) which this filter rule will apply to. **Source/Destination Port -**

(=) – when the first and last value are the same, it indicates one port; when the first and last values are different, it indicates a range for the port and available for this service type.

(*!=*) – when the first and last value are the same, it indicates all the ports except the port defined here; when the first and last values are different, it indicates that all the ports except the range defined here are available for this service type.

(>) – the port number greater than this value is available.

(<) – the port number less than this value is available for this profile.

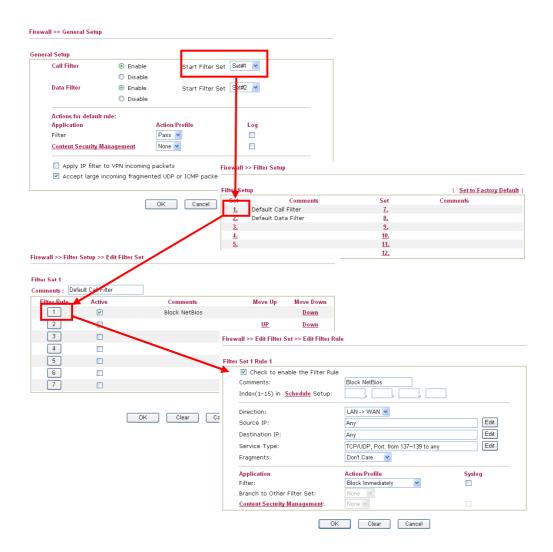
Service Group/Object - Use the drop down list to choose the one that you want.

Fragments Specify the action for fragmented packets. And it is used for Data Filter only. **Don't care** - No action will be taken towards fragmented packets. Unfragmented - Apply the rule to unfragmented packets. *Fragmented* - Apply the rule to fragmented packets. Too Short - Apply the rule only to packets that are too short to contain a complete header. Filter Specifies the action to be taken when packets match the rule. Block Immediately - Packets matching the rule will be dropped immediately. Pass Immediately - Packets matching the rule will be passed immediately. Block If No Further Match - A packet matching the rule, and that does not match further rules, will be dropped. Pass If No Further Match - A packet matching the rule, and that does not match further rules, will be passed through.

	For troubleshooting needs, you can specify to record Filter information by checking the Syslog box. It will be sent to Syslog server. Please refer to section 3.14.4 Syslog/Mail Alert for more detailed information.
Branch to other Filter Set	If the packet matches the filter rule, the next filter rule will branch to the specified filter set. Select next filter rule to branch from the drop-down menu. Be aware that the router will apply the specified filter rule for ever and will not return to previous filter rule any more.
IP Address	Specify a source and destination IP address for this filter rule to apply to. Place the symbol "!" before a specific IP Address will prevent this rule from being applied to that IP address. To apply the rule to all IP address, enter any or leave the field blank.
Content Management	All the hosts within the range configured with above conditions must follow the standard configured in the CSM profile (configured in Objects and Groups>>CSM Profiles) selected here. Please choose one of the CSM profiles applied by this filter rule.
	For troubleshooting needs, you can specify to record CSM information by checking the Syslog box. It will be sent to Syslog server. Please refer to section 3.14.4 Syslog/Mail Alert for more detailed information.

Example

As stated before, all the traffic will be separated and arbitrated using on of two IP filters: call filter or data filter. You may preset 12 call filters and data filters in **Filter Setup** and even link them in a serial manner. Each filter set is composed by 7 filter rules, which can be further defined. After that, in **General Setup** you may specify one set for call filter and one set for data filter to execute first.



3.5.4 DoS Defense

As a sub-functionality of IP Filter/Firewall, there are 15 types of detect/ defense function in the **DoS Defense** setup. The DoS Defense functionality is disabled for default.

Click Firewall and click DoS Defense to open the setup page.

Firewall >> DoS defense Setup		1	110				
DoS defense Setup							
Enable DoS Defense							
Enable SYN flood defen	se	Threshold	50	packets / sec			
		Timeout	10	sec			
Enable UDP flood defen:	5e	Threshold	150	packets / sec			
		Timeout	10	sec			
🔲 Enable ICMP flood defer	ise	Threshold	50	packets / sec			
		Timeout	10	sec			
🗌 Enable Port Scan detec	tion	Threshold	150	packets / sec			
🔲 Block IP options		🔲 Block TCP fl	lag scan				
Block Land		📃 Block Tear (🗌 Block Tear Drop				
Block Smurf		🔲 Block Ping o	of Death				
Block trace route		🔲 Block ICMP	fragment				
Block SYN fragment		🔲 Block Unkno	wnProtocol				
📃 Block Fraggle Attack							
Enable DoS defens crackers.	≥ function to pr	event the attacks	from hacke	r or 🔨			
Enable Dos Defense Enable SYN flood defense	Check the b detecting th Internet has to randomly period defin SYN packet router. By o packets per	y discard the su ned in Timeout ets' attempt to e default, the thre second and 10	the SYN f the TCP S defined va bsequent ' . The goal xhaust the shold and seconds, t	lood defense fu SYN packets fr lue, the Vigor : TCP SYN pack for this is prev limited-resoun timeout values respectively.	anction. Once rom the router will start cets for a vent the TCP rce of Vigor s are set to 50		
Enable UDP flood defense	detecting the exceeded the randomly defined in 7	box to activate the Threshold of the defined value discard the subsection of the sub	the UDP e, the Vigo equent UI efault setti	packets from the packets from the packets for a packets for a for threshold by the packets for	he Internet has tart to a period ld and timeout		
Enable ICMP flood defense	Similar to t of ICMP pa router will Internet. Th	box to activate the UDP flood of ackets from Internet discard the ICM are default setting second and 10	defense fur ernet has e AP echo re g for thres	nction, once if xceeded the de equests coming shold and time	the Threshold fined value, the from the		
Enable PortScan detection	many ports Check the b	ttacks the Vigo in an attempt to box to activate this malicious ex	o find igno the Port So	orant services v can detection. V	would respond. Whenever		

	port-scanning Threshold rate, the Vigor router will send out a warning. By default, the Vigor router sets the threshold as 150 packets per second.
Block IP options	Check the box to activate the Block IP options function. The Vigor router will ignore any IP packets with IP option field in the datagram header. The reason for limitation is IP option appears to be a vulnerability of the security for the LAN because it will carry significant information, such as security, TCC (closed user group) parameters, a series of Internet addresses, routing messagesetc. An eavesdropper outside might learn the details of your private networks.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed SYN packets with the identical source and destination addresses, as well as the port number to victims.
Block Smurf	Check the box to activate the Block Smurf function. The Vigor router will ignore any broadcasting ICMP echo request.
Block trace router	Check the box to enforce the Vigor router not to forward any trace route packets.
Block SYN fragment	Check the box to activate the Block SYN fragment function. The Vigor router will drop any packets having SYN flag and more fragment bit set.
Block Fraggle Attack	Check the box to activate the Block fraggle Attack function. Any broadcast UDP packets received from the Internet is blocked. Activating the DoS/DDoS defense functionality might block some legal packets. For example, when you activate the fraggle attack defense, all broadcast UDP packets coming from the Internet are blocked. Therefore, the RIP packets from the Internet might be dropped.
Block TCP flag scan	Check the box to activate the Block TCP flag scan function. Any TCP packet with anomaly flag setting is dropped. Those scanning activities include <i>no flag scan</i> , <i>FIN without ACK scan</i> , <i>SYN FINscan</i> , <i>Xmas scan</i> and <i>full Xmas scan</i> .
Block Tear Drop	Check the box to activate the Block Tear Drop function. Many machines may crash when receiving ICMP datagrams (packets) that exceed the maximum length. To avoid this type of attack, the Vigor router is designed to be capable of discarding any fragmented ICMP packets with a length greater than 1024 octets.
Block Ping of Death	Check the box to activate the Block Ping of Death function. This attack involves the perpetrator sending overlapping packets to the target hosts so that those target hosts will hang once they re-construct the packets. The Vigor routers will block any packets realizing this attacking activity.
Block ICMP Fragment	Check the box to activate the Block ICMP fragment function. Any ICMP packets with more fragment bit set are dropped.
Block Land	Check the box to enforce the Vigor router to defense the Land attacks. The Land attack combines the SYN attack technology with IP spoofing. A Land attack occurs when an attacker sends spoofed

SYN packets with the identical source and destination addresses, as well as the port number to victims.

Block UnknownCheck the box to activate the Block Unknown Protocol function.ProtocolIndividual IP packet has a protocol field in the datagram header to
indicate the protocol type running over the upper layer. However,
the protocol types greater than 100 are reserved and undefined at
this time. Therefore, the router should have ability to detect and
reject this kind of packets.

Warning Messages We provide Syslog function for user to retrieve message from Vigor router. The user, as a Syslog Server, shall receive the report sending from Vigor router which is a Syslog Client.

All the warning messages related to **DoS defense** will be sent to user and user can review it through Syslog daemon. Look for the keyword **DoS** in the message, followed by a name to indicate what kind of attacks is detected.

SysLog Access Setup	Mail Alert Setup	
🗹 Enable	🔲 Enable	
Server IP Address 192.168.1.115	SMTP Server	
Destination Port 514	Mail To	
Enable syslog message:	Return-Path	
🔲 Firewall Log	Authentication	
VPN Log	User Name	
User Access Log		
🔲 Call Log	Password	
WAN Log		
Router/DSL information		

🕅 DrayTek Syslog				
Controls	192.168.1.1 Vigor 3100 series Dmt.Bis	WAN Status Getway IP (Fixed)	TX Packets	RX Rate
931	1182		0	0
Firewall Log VPN Log	Uzer Access Log Call Log WAN L	og Budget Log Network	Infomation Net Stat	e
Time Host	Message			
Jan 1 00:00:42 Vigor Jan 1 00:00:34 Vigor	DoS syn_flood Block(10s) 192.168 DoS icmp_flood Block(10s) 192.164	1.115,10605 → 192,168.1 8.1.115 → 192,168.1.1 PR 1	,23 PR 6(tcp) len 20 4 (icmp) len 20 60 icmp	10 - 8 3943751 9 0/8
<				>
ADSL Status Mode T1.413	State Up Speed HANDSHAKE 0	Down Speed	SNR Margin	Loop Att 0.0

3.5.5 URL Content Filter

Based on the list of user defined keywords, the URL Content Filter facility in Vigor router inspects the URL string in every outgoing HTTP request. No matter the URL string is found full or partial matched with a keyword, the Vigor router will block the associated HTTP connection.

For example, if you add key words such as "sex", Vigor router will limit web access to web sites or web pages such as "www.sex.com", "www.backdoor.net/images/sex/p_386.html". Or you may simply specify the full or partial URL such as "www.sex.com" or "sex.com".

Also the Vigor router will discard any request that tries to retrieve the malicious code.

Click Firewall and click URL Content Filter to open the setup page.

Content Filter S	etup		
Enable URL	Access Control		
Enable U	RL Access Log		
	t (block those matching keyword)		
🔘 White Lis	t (pass those matching keyword)		
No ACT	Keyword	No ACT	Keyword
1		5 🔲	
2		6 🔲	
3 🔲		7	
4		8 🔲	
Note that r	nultiple keywords are allowed to spe	ecify in the blank	For example: hotmail yahoo msn
	b access from IP address	,	
	Proxy	~ ~	Subnet Mask
3		~	
4		~	
Time Schedule			
Index(1-15)	n <u>Schedule</u> Setup:,	,,	
Note: Action a	nd Idle Timeout settings will be igno	ored.	
	ОК СІ	lear All 🛛 Can	cel
Enable UR Control	L Access Check the b	ox to activa	te URL Access Control.
Black List natching k			rict accessing into the correspon ords listed on the box below.

Firewall >> URL Content Filter

White List (pass those Click this button to allow accessing into the corresponding webpage with the keywords listed on the box below.

Keyword The Vigor router provides 8 frames for users to define keywords and each frame supports multiple keywords. The keyword could be a noun, a partial noun, or a complete URL string. Multiple keywords within a frame are separated by space, comma, or semicolon. In addition, the maximal length of each frame is 32-character long. After specifying keywords, the Vigor router will

matching keyword)

	decline the connection request to the website whose URL string matched to any user-defined keyword. It should be noticed that the more simplified the blocking keyword list, the more efficiently the Vigor router perform.
Prevent web access from IP address	Check the box to deny any web surfing activity using IP address, such as http://202.6.3.2. The reason for this is to prevent someone dodges the URL Access Control.
	You must clear your browser cache first so that the URL content filtering facility operates properly on a web page that you visited before.
Enable Restrict Web Feature	Check the box to activate the function. <i>Java</i> - Check the checkbox to activate the Block Java object function. The Vigor router will discard the Java objects from the Internet.
	<i>ActiveX</i> - Check the box to activate the Block ActiveX object function. Any ActiveX object from the Internet will be refused. <i>Compressed file</i> - Check the box to activate the Block Compressed file function to prevent someone from downloading any compressed file. The following list shows the types of compressed files that can be blocked by the Vigor router zip, rar, .arj, .ace, .cab, .sit
	<i>Executable file</i> - Check the box to reject any downloading behavior of the executable file from the Internet. .exe, .com, .scr, .pif, .bas, .bat, .inf, .reg
	 Cookie - Check the box to filter out the cookie transmission from inside to outside world to protect the local user's privacy. Proxy - Check the box to reject any proxy transmission. To control efficiently the limited-bandwidth usage, it will be of great value to provide the blocking mechanism that filters out the multimedia files downloading from web pages. Accordingly, files with the following extensions will be blocked by the Vigor router. .mov .mp3 .rm .ra .au .wmv
	.wav .asf .mpg .mpeg .avi .ram
Enable Excepting Subnets	Four entries are available for users to specify some specific IP addresses or subnets so that they can be free from the <i>URL Access Control</i> . To enable an entry, click on the empty checkbox, named as ACT , in front of the appropriate entry.
Time Schedule	Specify what time should perform the URL content filtering facility.

3.5.6 Web Content Filter

Click Firewall and click Web Content Filter to open the setup page.

For this section, please refer to **Web Content Filter** user's guide.

Firewall >> Web Content Filter Setup

CPA(Content Portal Authority) Web Content Filter Setup					
Select a CPA server: asia site Activate Free Trial and Purchase Subscription Check the Validity Test a site to verify whether it is categorized					
Enable Web Content F					
Groups	Categories (Tick categor	ies to block. Untick to unl	block)		
Child Protection Select All Clear All	Chat Gambling Sex	Criminal Hacking Violence	Drugs/Alcohol Hate speech Weapons		
Leisure Select All Clear All	Advertisements Games Hobbies Personals Sports	Entertainment Glamour Lifestyle Photo Searches Streaming Media	 Food Health Motor Vehicles Shopping Travel 		
Business Select All Clear All	Computing/Internet Politics Remote proxies	☐ Finance ☐ Real Estate ☐ Search Engine	☐ Job Search/Career ☐ Reference ☐ Web Mail		
Others Select All Clear All	 Education News Usenet news 	☐ Hosting sites ☐ Religion ☐ Block all uncategorise	Cites Sex Education disites		
Time Schedule Index(1-15) in Schedule Setup: , , , Note: Action and Idle Timeout settings will be ignored.					
	ОК	Cancel			

3.6 Bandwidth Management

Below shows the menu items for Bandwidth Management.

- Bandwidth Management

 Sessions Limit
 Bandwidth Limit
 - Quality of Service

3.6.1 Sessions Limit

A PC with private IP address can access to the Internet via NAT router. The router will generate the records of NAT sessions for such connection. The P2P (Peer to Peer) applications (e.g., BitTorrent) always need many sessions for procession and also they will occupy over resources which might result in important accesses impacted. To solve the problem, you can use limit session to limit the session procession for specified Hosts.

In the Bandwidth Management menu, click Sessions Limit to open the web page.

С) Enabl	le 💿 Disable					
De	efault M	1ax Sessions: 100					
Lii	nitatio	n List					
I	ndex	Start IP	End	IP	Max	Sessions	
St	art IP:			End IP:			
Ma	aximum	Sessions:	Add	Edit	Delete		
e Schedu	le						
Index(1	-15) in	Setup:	,	,,	,		
Note: A	ction a	nd Idle Timeout set	tings wil	ll be ignore	d.		

Bandwidth Management >> Sessions Limit

To activate the function of limit session, simply click **Enable** and set the default session limit.

Enable	Click this button to activate the function of limit session.
Disable	Click this button to close the function of limit session.
Default session limit	Defines the default session number used for each computer in LAN.
Limitation List	Displays a list of specific limitations that you set on this web page.
Start IP	Defines the start IP address for limit session.
End IP	Defines the end IP address for limit session.

Maximum Sessions	Defines the available session number for specific range of IP addresses. If you do not set the session number in this field, the system will use the default session limit for the specific limitation you set for each index.
Add	Adds the specific session limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

3.6.2 Bandwidth Limit

Bandwidth Management >> Limit Bandwidth

The downstream or upstream from FTP, HTTP or some P2P applications will occupy large of bandwidth and affect the applications for other programs. Please use Limit Bandwidth to make the bandwidth usage more efficient.

In the **Bandwidth Management** menu, click **Bandwidth Limit** to open the web page.

🔘 Enabl	e 💿 Disable					
Default T	× Limit: 0	Kbps	Default R>	: Limit: 0		Kbps
Limitatior						
Index	Start IP	End	IP	ТХ	limit	RXlimit
Specific L	imitation					
Specific L Start IP:	imitation		End IP:			
		RX Limit Add	t:	Kbps Delete		
Start IP:			t:			
Start IP: TX Limit: hedule		Add	t:			

To activate the function of limit bandwidth, simply click **Enable** and set the default upstream and downstream limit.

OK

Click this button to activate the function of limit bandwidth.
Click this button to close the function of limit bandwidth.
Define the default speed of the upstream for each computer in LAN.
Define the default speed of the downstream for each computer in LAN.

Limitation List	Display a list of specific limitations that you set on this web page.
Start IP	Define the start IP address for limit bandwidth.
End IP	Define the end IP address for limit bandwidth.
TX limit	Define the limitation for the speed of the upstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
RX limit	Define the limitation for the speed of the downstream. If you do not set the limit in this field, the system will use the default speed for the specific limitation you set for each index.
Add	Add the specific speed limitation onto the list above.
Edit	Allows you to edit the settings for the selected limitation.
Delete	Remove the selected settings existing on the limitation list.
Index (1-15) in Schedule Setup	You can type in four sets of time schedule for your request. All the schedules can be set previously in Application – Schedule web page and you can use the number that you have set in that web page.

3.6.3 Quality of Service

Deploying QoS (Quality of Service) management to guarantee that all applications receive the service levels required and sufficient bandwidth to meet performance expectations is indeed one important aspect of modern enterprise network.

One reason for QoS is that numerous TCP-based applications tend to continually increase their transmission rate and consume all available bandwidth, which is called TCP slow start. If other applications are not protected by QoS, it will detract much from their performance in the overcrowded network. This is especially essential to those are low tolerant of loss, delay or jitter (delay variation).

Another reason is due to congestions at network intersections where speeds of interconnected circuits mismatch or traffic aggregates, packets will queue up and traffic can be throttled back to a lower speed. If there's no defined priority to specify which packets should be discarded (or in another term "dropped") from an overflowing queue, packets of sensitive applications mentioned above might be the ones to drop off. How this will affect application performance?

There are two components within Primary configuration of QoS deployment:

- Classification: Identifying low-latency or crucial applications and marking them for high-priority service level enforcement throughout the network.
- Scheduling: Based on classification of service level to assign packets to queues and associated service types

The basic QoS implementation in Vigor routers is to classify and schedule packets based on the service type information in the IP header. For instance, to ensure the connection with the headquarter, a teleworker may enforce an index of QoS Control to reserve bandwidth for HTTPS connection while using lots of application at the same time.

One more larger-scale implementation of QoS network is to apply DSCP (Differentiated Service Code Point) and IP Precedence disciplines at Layer 3. Compared with legacy IP Precedence that uses Type of Service (ToS) field in the IP header to define 8 service classes, DSCP is a successor creating 64 classes possible with backward IP Precedence compatibility.

In a QoS-enabled network, or Differentiated Service (DiffServ or DS) framework, a DS domain owner should sign a Service License Agreement (SLA) with other DS domain owners to define the service level provided toward traffic from different domains. Then each DS node in these domains will perform the priority treatment. This is called per-hop-behavior (PHB). The definition of PHB includes Expedited Forwarding (EF), Assured Forwarding (AF), and Best Effort (BE). AF defines the four classes of delivery (or forwarding) classes and three levels of drop precedence in each class.

Vigor routers as edge routers of DS domain shall check the marked DSCP value in the IP header of bypassing traffic, thus to allocate certain amount of resource execute appropriate policing, classification or scheduling. The core routers in the backbone will do the same checking before executing treatments in order to ensure service-level consistency throughout the whole QoS-enabled network.



However, each node may take different attitude toward packets with high priority marking since it may bind with the business deal of SLA among different DS domain owners. It's not easy to achieve deterministic and consistent high-priority QoS traffic throughout the whole network with merely Vigor router's effort.

In the Bandwidth Management menu, click Quality of Service to open the web page.

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setur</u>
Class Ri Inde		N	ame				Rule	Service	Туре
	эх	N	ame				Rule <u>Edit</u>	Service	Туре
Inde	9X 5 1	N	ame					Service <u>Edit</u>	

Bandwidth Management >> Quality of Service

This page displays the QoS settings result of the WAN interface. Click the **Setup** link to access into next page for the general setup of WAN (1/2) interface. As to class rule, simply click the **Edit** link to access into next for configuration.

You can configure general setup for the WAN interface, edit the Class Rule, and edit the Service Type for the Class Rule for your request.

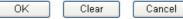
General Setup for WAN Interface

When you click **Setup**, you can configure the bandwidth ratio for QoS of the WAN interface. There are four queues allowed for QoS control. The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. Yet, the last one is reserved for the packets which are not suitable for the user-defined class rules.

Bandwidth Management >> Quality of Service

WAN1 General Setup

🗹 Enable the C	loS Control OUT 🔽	
	WAN Inbound Bandwidth	10000 Kbps
	WAN Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1		25 %
Class 2		25 %
Class 3		25 %
	Others	25 %
	Bandwidth Control CP ACK Prioritize	Limited_bandwidth Ratio 25 % <u>Online Statistics</u>

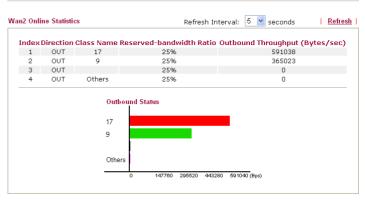


Enable the QoS Control	 The factory default for this setting is checked. Please also define which traffic the QoS Control settings will apply to. IN- apply to incoming traffic only. OUT-apply to outgoing traffic only. BOTH- apply to both incoming and outgoing traffic. Check this box and click OK, then click Setup link again. You will see the Online Statistics link appearing on this page.
WAN Inbound Bandwidth	It allows you to set the connecting rate of data input for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 10000kbps for this box. The default value is 10000kbps.
WAN Outbound Bandwidtl	h It allows you to set the connecting rate of data output for WAN. For example, if your ADSL supports 1M of downstream and 256K upstream, please set 256kbps for this box. The default value is 10000kbps.
Reserved Bandwidth Ratio	It is reserved for the group index in the form of ratio of reserved bandwidth to upstream speed and reserved bandwidth to downstream speed .
Enable UDP Bandwidth Control	Check this and set the limited bandwidth ratio on the right field. This is a protection of TCP application traffic since UDP application traffic such as streaming video will exhaust lots of bandwidth.
Outbound TCP ACK Prioritize	The difference in bandwidth between download and upload are great in ADSL2+ environment. For the download speed might be impacted by the uploading TCP ACK, you can check this box to push ACK of upload more faster to speed the network traffic.
Limited_bandwidth Ratio	The ratio typed here is reserved for limited bandwidth of UDP application.

On Line Statistics

Display an online statistics for quality of service for your reference.

Bandwidth Management >> Quality of Service



Edit the Class Rule for QoS

The first three (Class 1 to Class 3) class rules can be adjusted for your necessity. To add, edit or delete the class rule, please click the **Edit** link of that one.

Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setu</u>

Class 1 Edit Class 2 Edit Class 3 Edit	Index	Name	Rule	Service Type
	Class 1		<u>Edit</u>	
Class 3 Edit	Class 2		<u>Edit</u>	<u>Edit</u>
	Class 3		<u>Edit</u>	

After you click the **Edit** link, you will see the following page. Now you can define the name for that Class. In this case, "Test" is used as the name of Class Index #1.

Bandwidth Management >> Quality of Service

Vame	test							
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type			
1 🔿	Active	Any	Any	ANY	ANY			
	Add Edit Delete							

For adding a new rule, click **Add** to open the following page.

rule.

Bandwidth Management >> Quality of Service

🗹 ACT		
Local Address	Any	
Remote Address	Any	
DiffServ CodePoint	ANY	~
Service Type	ANY	*
Note: Please choose/se	tup the <u>Service Type</u>	first.

OK Cancel

ACT

Check this box to invoke these settings.

Click the **SrcEdit** button to set the source address for the rule. Click the **DestEdit** button to set the destination address for the

Destination Address

Source Address

SrcEdit/DestEdit

It allows you to edit source address information.

Address Type	Subnet Address 💌
Start IP Address	0.0.0.0
End IP Address	0.0.0.0
Subnet Mask	0.0.0.0

Address Type – Determine the address type for the source address.

For **Single Address**, you have to fill in Start IP address. For **Range Address**, you have to fill in Start IP address and End IP address.

For **Subnet Address**, you have to fill in Start IP address and Subnet Mask.

DiffServ CodePointAll the packets of data will be divided with different levels
and will be processed according to the level type by the
system. Please assign one of the level of the data for
processing with QoS control.Service TypeIt determines the service type of the data for processing with
QoS control. It can also be edited. You can choose the
predefined service type from the Service Type drop down list.
Those types are predefined in factory. Simply choose the one
that you want for using by current QoS.

By the way, you can set up to 20 rules for one Class. If you want to edit an existed rule, please select the radio button of that one and click **Edit** to open the rule edit page for modification.

ne	Game					
NO	Status	Local Address	Remote Address	DiffServ CodePoint	Service Type	
1 ()	Active	Any	Any	IP precedence 2	SYSLOG(UDP:514)	
2 🔿	Active	192.168.1.15	AF Class1 (Low Drop)	FTP(TCP:20)		
Add Edit Delete						

Edit the Service Type for Class Rule

To add a new service type, edit or delete an existed service type, please click the Edit link under Service Type field.

Bandwidth Management >> Quality of Service

Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setu

Index	Name	Rule	Service Type
Class 1		<u>Edit</u>	
Class 2		<u>Edit</u>	<u>Edit</u>
Class 3		<u>Edit</u>	

After you click the Edit link, you will see the following page.

ser Defined Service Type			
NO	Name	Protocol	Port
1	Empty	-	-
		Add Edit Delete	

For adding a new rule, click **Add** to open the following page. If you want to edit an existed service type, please select the radio button of that one and click **Edit** to open the following page for modification.

Bandwidth Management >> Quality of Service

Service Type Edit		
Service Name		
Service Type		TCP 🖌 6
Port Configura	ation	
Туре		💿 Single 🛛 Range
Port Nu	mber	0 - 0
	Oł	K Cancel
Service Name	Type in a	new service for your request.
Service Type	Choose th service.	ne type (TCP, UDP or TCP/UDP) for the new
Port Configuration	in the star boxes bel	gle or Range . If you select Range, you have to type rting port number and the end porting number on the low. nber – Type in the starting port number and the end
		umber here if you choose Range as the type.

By the way, you can set up to 40 service types. If you want to edit/delete an existed service type, please select the radio button of that one and click **Edit/Edit** for modification.

3.7 Applications

Below shows the menu items for Applications.

Applications	
Dynamic DNS	
Schedule	
RADIUS	
▶ UPnP	
Wake on LAN	

3.7.1 Dynamic DNS

The ISP often provides you with a dynamic IP address when you connect to the Internet via your ISP. It means that the public IP address assigned to your router changes each time you access the Internet. The Dynamic DNS feature lets you assign a domain name to a dynamic WAN IP address. It allows the router to update its online WAN IP address mappings on the specified Dynamic DNS server. Once the router is online, you will be able to use the registered domain name to access the router or internal virtual servers from the Internet. It is particularly helpful if you host a web server, FTP server, or other server behind the router.

Before you use the Dynamic DNS feature, you have to apply for free DDNS service to the DDNS service providers. The router provides up to three accounts from three different DDNS service providers. Basically, Vigor routers are compatible with the DDNS services supplied by most popular DDNS service providers such as **www.dyndns.org**, **www.no-ip.com**, **www.dtdns.com**, **www.changeip.com**, **www.dynamic- nameserver.com**. You should visit their websites to register your own domain name for the router.

Enable the Function and Add a Dynamic DNS Account

- 1. Assume you have a registered domain name from the DDNS provider, say *hostname.dyndns.org*, and an account with username: *test* and password: *test*.
- 2. In the DDNS setup menu, check Enable Dynamic DNS Setup.

Applications >> Dynamic DNS Setup		

Dynamic DNS Setup		I	Set to Factory Default
Enable Dynamic DNS Setup		View Log	Force Update
Accounts :			
Index	WAN Interface	Domain Name	Active
<u>1.</u>	WAN1 First		х
<u>2.</u>	WAN1 First		×
<u>3.</u>	WAN1 First		×



Set to Factory DefaultClear all profiles and recover to factory settings.Enable Dynamic DNS SetupCheck this box to enable DDNS function.IndexClick the number below Index to access into the setting page of DDNS setup to set account(s).WAN InterfaceDisplay current WAN interface used for accessing Internet.

Domain Name	Display the domain name that you set on the setting page of DDNS setup.
Active	Display if this account is active or inactive.
View Log	Display DDNS log status.
Force Update	Force the router updates its information to DDNS server.

3. Select Index number 1 to add an account for the router. Check Enable Dynamic DNS Account, and choose correct Service Provider: dyndns.org, type the registered hostname: *hostname* and domain name suffix: dyndns.org in the Domain Name block. The following two blocks should be typed your account Login Name: *test* and Password: *test*.

Applications >> Dynamic DNS Setup >> Dynamic DNS Account Setup

ΟK

Index:1 🗹 Enable Dynamic DNS Account WAN Interface WAN1 First 🔽 Service Provider dyndns.org (www.dyndns.org) ¥ Service Type Dynamic 🔽 chronic6853 Domain Name dyndns.info dyndns.info v Login Name chronic6853 (max. 23 characters) Password (max. 23 characters) Wildcards 📃 Backup MX Mail Extender

Clear

Cancel

Enable Dynamic DNS Account	Check this box to enable the current account. If you did check the box, you will see a check mark appeared on the Active column of the previous web page in step 2).
WAN Interface	Select the WAN interface order to apply settings here.
Service Provider	Select the service provider for the DDNS account.
Service Type	Select a service type (Dynamic, Custom, Static). If you choose Custom, you can modify the domain that is choosen in the Domain Name field.
Domain Name	Type in a domain name that you applied previously. Use the drop down list to choose the desired domain.
Login Name	Type in the login name that you set for applying domain.
Password	Type in the password that you set for applying domain.
Clinita OV harden and a set	

4. Click **OK** button to activate the settings. You will see your setting has been saved.

The Wildcard and Backup MX features are not supported for all Dynamic DNS providers. You could get more detailed information from their websites.

Disable the Function and Clear all Dynamic DNS Accounts

In the DDNS setup menu, uncheck **Enable Dynamic DNS Setup**, and push **Clear All** button to disable the function and clear all accounts from the router.

Delete a Dynamic DNS Account

In the DDNS setup menu, click the **Index** number you want to delete and then push **Clear All** button to delete the account.

3.7.2 Schedule

The Vigor router has a built-in real time clock which can update itself manually or automatically by means of Network Time Protocols (NTP). As a result, you can not only schedule the router to dialup to the Internet at a specified time, but also restrict Internet access to certain hours so that users can connect to the Internet only during certain hours, say, business hours. The schedule is also applicable to other functions.

You have to set your time before set schedule. In **System Maintenance>> Time and Date** menu, press **Inquire Time** button to set the Vigor router's clock to current time of your PC. The clock will reset once if you power down or reset the router. There is another way to set up time. You can inquiry an NTP server (a time server) on the Internet to synchronize the router's clock. This method can only be applied when the WAN connection has been built up.

ule:			Set to Factory Def
Index	Status	Index	Status
<u>1.</u>	х	<u>9.</u>	х
<u>2.</u>	х	<u>10.</u>	х
<u>3.</u>	х	<u>11.</u>	х
<u>4.</u>	x	<u>12.</u>	х
<u>5.</u>	х	<u>13.</u>	х
<u>6.</u>	х	<u>14.</u>	х
<u>7.</u>	х	<u>15.</u>	х
<u>8.</u>	×		

Applications	>>	Schedule
Applications		Schedule

Status: v --- Active, x --- Inactive

Set to Factory Default	Clear all profiles and recover to factory settings.
Index	Click the number below Index to access into the setting page of schedule.
Status	Display if this schedule setting is active or inactive.

You can set up to 15 schedules. Then you can apply them to your **Internet Access** or **VPN** and **Remote Access** >> **LAN-to-LAN** settings.

To add a schedule, please click any index, say Index No. 1. The detailed settings of the call schedule with index 1 are shown below.

Applications >> Schedule

ndex No. 1		
🗹 Enable 🤅	Schedule Setup	
	Start Date (yyyy-mm-dd)	2000 🗸 1 🖌 1 🔽
	Start Time (hh:mm)	0 🛩 : 0 🛩
	Duration Time (hh:mm)	
	Action	Force On
	Idle Timeout	minute(s).(max. 255, 0 for default)
	How Often	
	O Once	
	💿 Weekdays	
	🗌 Sun 🗹 Mon 🗹	Tue 🗹 Wed 🗹 Thu 🗹 Fri 🔲 Sat

Enable Schedule Setup	Check to enable the schedule.
Start Date (yyyy-mm-dd)	Specify the starting date of the schedule.
Start Time (hh:mm)	Specify the starting time of the schedule.
Duration Time (hh:mm)	Specify the duration (or period) for the schedule.
Action	 Specify which action Call Schedule should apply during the period of the schedule. Force On -Force the connection to be always on. Force Down -Force the connection to be always down. Enable Dial-On-Demand -Specify the connection to be dial-on-demand and the value of idle timeout should be specified in Idle Timeout field. Disable Dial-On-Demand -Specify the connection to be up when it has traffic on the line. Once there is no traffic over idle timeout, the connection will be down and never up again during the schedule.
Idle Timeout	Specify the duration (or period) for the schedule. How often -Specify how often the schedule will be applied Once -The schedule will be applied just once Weekdays -Specify which days in one week should perform the schedule.

Example

Suppose you want to control the PPPoE Internet access connection to be always on (Force On) from 9:00 to 18:00 for whole week. Other time the Internet access connection should be disconnected (Force Down).



- 1. Make sure the PPPoE connection and **Time Setup** is working properly.
- 2. Configure the PPPoE always on from 9:00 to 18:00 for whole week.

- 3. Configure the **Force Down** from 18:00 to next day 9:00 for whole week.
- Assign these two profiles to the PPPoE Internet access profile. Now, the PPPoE Internet connection will follow the schedule order to perform Force On or Force Down action according to the time plan that has been pre-defined in the schedule profiles.

3.7.3 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting, which is widely used by Internet service providers. It is the most common method of authenticating and authorizing dial-up and tunneled network users.

The built-in RADIUS client feature enables the router to assist the remote dial-in user or a wireless station and the RADIUS server in performing mutual authentication. It enables centralized remote access authentication for network management.

Applications >> RADIUS		
RADIUS Setup		
🗹 Enable		
Server IP	Address	
Destinatio	n Port 1812	
Shared Se	acret	
Confirm Sł	hared Secret	
	OK Clear Cancel	
Enable	Check to enable RADIUS client feature	
Server IP Address	Enter the IP address of RADIUS server	
Destination Port	The UDP port number that the RADIUS server is using. The default value is 1812, based on RFC 2138.	
Shared Secret	The RADIUS server and client share a secret that is used to authenticate the messages sent between them. Both sides must be configured to use the same shared secret.	
Confirm Shared Secret	Re-type the Shared Secret for confirmation.	

3.7.4 UPnP

The **UPnP** (Universal Plug and Play) protocol is supported to bring to network connected devices the ease of installation and configuration which is already available for directly connected PC peripherals with the existing Windows 'Plug and Play' system. For NAT routers, the major feature of UPnP on the router is "NAT Traversal". This enables applications inside the firewall to automatically open the ports that they need to pass through a router. It is more reliable than requiring a router to work out by itself which ports need to be opened. Further, the user does not have to manually set up port mappings or a DMZ. **UPnP is available on Windows XP** and the router provides the associated support for MSN Messenger to allow full use of the voice, video and messaging features.

Applications >> UPnP

UPnP	
🗹 Enable UPnP Servi	ce
	Enable Connection control Service
	Enable Connection Status Service

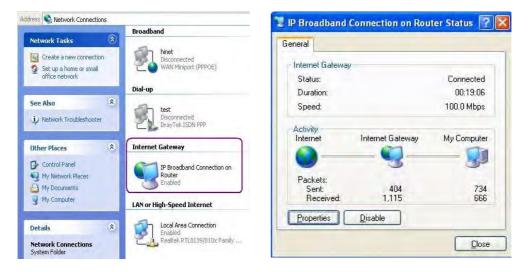
Note: If you intend running UPnP service inside your LAN, you should check the appropriate service above to allow control, as well as the appropriate UPnP settings.



Enable UPNP Service

Accordingly, you can enable either the **Connection Control Service** or **Connection Status Service**.

After setting **Enable UPNP Service** setting, an icon of **IP Broadband Connection on Router** on Windows XP/Network Connections will appear. The connection status and control status will be able to be activated. The NAT Traversal of UPnP enables the multimedia features of your applications to operate. This has to manually set up port mappings or use other similar methods. The screenshots below show examples of this facility.



The UPnP facility on the router enables UPnP aware applications such as MSN Messenger to discover what are behind a NAT router. The application will also learn the external IP address and configure port mappings on the router. Subsequently, such a facility forwards packets from the external ports of the router to the internal ports used by the application.

eneral	Services
Connect to the Internet using:	Select the services running on your network that Internet users can access.
S IP Broadband Connection on Router	Services
This connection allows you to connect to the Internet through a chared connection on another computer.	 Ftp Example msnmsgr (192.168.29.11:13135) 60654 UDP msnmsgr (192.168.29.11:7824) 13251 UDP msnmsgr (192.168.29.11:8789) 63231 TCP

The reminder as regards concern about Firewall and UPnP

Can't work with Firewall Software

Enabling firewall applications on your PC may cause the UPnP function not working properly. This is because these applications will block the accessing ability of some network ports.

Security Considerations

Activating the UPnP function on your network may incur some security threats. You should consider carefully these risks before activating the UPnP function.

- Some Microsoft operating systems have found out the UPnP weaknesses and hence you need to ensure that you have applied the latest service packs and patches.
- Non-privileged users can control some router functions, including removing and adding port mappings.

The UPnP function dynamically adds port mappings on behalf of some UPnP-aware applications. When the applications terminate abnormally, these mappings may not be removed.

3.7.5 Wake On LAN

A PC client on LAN can be woken up by the router it connects. When a user wants to wake up a specified PC through the router, he/she must type correct MAC address of the specified PC on this web page of **Wake On LAN** of this router.

In addition, such PC must have installed a network card supporting WOL function. By the way, WOL function must be set as "Enable" on the BIOS setting.

Application >> Wake on LAN

Note: Wake on L can wake up thr	AN cooperate with <u>Bind IP to MAC</u> function, only binded PCs ough IP.
Wake by:	MAC Address 💌
IP Address:	😵
MAC Address:	Wake Up!
Result	
	<u>^</u>

Wake by	choose Wake by MAC MAC address of the he	you to wake up the binded IP. If you Address, you have to type the correct ost in MAC Address boxes. If you dress, you have to choose the correct IP
	Wake by:	MAC Address V MAC Address IP Address
IP Address	Firewall>>Bind IP to	have been configured in MAC will be shown in this drop down ress from the drop down list that you
MAC Address	Type any one of the M	AC address of the binded PCs.
Wake Up	Click this button to wa figure. The result will	ke up the selected IP. See the following be shown on the box.

Note: Wake on L can wake up thr	AN cooperate with <u>Bind IP to MAC</u> function, only binded PCs ough IP.
Wake by:	MAC Address 💌
IP Address:	😒
MAC Address:	Wake Up!
Result	
Send command	to client done.

Application >> Wake on LAN

3.8 VPN and Remote Access

A Virtual Private Network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. In short, by VPN technology, you can send data between two computers across a shared or public network in a manner that emulates the properties of a point-to-point private link.

Besides, here provides ISDN LAN to LAN and remote dial-in functions (for *i* model only).

Below shows the menu items for VPN and Remote Access.

VPN and Remote Access
Remote Access Control
PPP General Setup
IPSec General Setup
IPSec Peer Identity
Remote Dial-in User
LAN to LAN
VPN TRUNK Management
Connection Management

3.8.1 Remote Access Control

Enable the necessary VPN service as you need. If you intend to run a VPN server inside your LAN, you should disable the VPN service of Vigor Router to allow VPN tunnel pass through, as well as the appropriate NAT settings, such as DMZ or open port. And, if you want to enable ISDN dial-in function, please check "Enable ISDN Dial-In" in this page.

Remote Access Control Setup		
	~	Enable PPTP VPN Service
		Enable IPSec VPN Service
		Enable L2TP VPN Service
		Enable ISDN Dial-In

Note: If you intend running a VPN server inside your LAN, you should uncheck the appropriate protocol above to allow pass-through, as well as the appropriate NAT settings.

OK	Clear	Cancel

Enable PPTP VPN Service	Check this box to activate the VPN service through PPTP protocol.
Enable IPSec VPN Service	Check this box to activate the VPN service through IPSec protocol.
Enable L2TP VPN Service	Check this box to activate the VPN service through L2TP protocol.
Enable ISDN Dial-IN	This feature is available for i model. Check this box to activate the ISDN dial-in.

3.8.2 PPP General Setup

This submenu only applies to PPP-related connections, such as PPTP, L2TP, L2TP over IPSec of VPN or ISDN.

VPN and Remote Access >> PPP General Setup

PPP General Setup			
PPP/MP Protocol		IP Address Assignment for Dial-	In Users
Dial-In PPP Authentication	PAP or CHAP	Start IP Address	192.168.1.200
Dial-In PPP Encryption (MPPE)	Optional MPPE		
Mutual Authentication	(PAP) (Yes 💿 No		
Username			
Password			

ОК

Dial-In PPP Authentication PAP Only	Select this option to force the router to authenticate dial-in users with the PAP protocol.
PAP or CHAP	Selecting this option means the router will attempt to authenticate dial-in users with the CHAP protocol first. If the dial-in user does not support this protocol, it will fall back to use the PAP protocol for authentication.
Dial-In PPP Encryption (MPPE Optional MPPE	This option represents that the MPPE encryption method will be optionally employed in the router for the remote dial-in user. If the remote dial-in user does not support the MPPE encryption algorithm, the router will transmit "no MPPE encrypted packets". Otherwise, the MPPE encryption scheme will be used to encrypt the data. Optional MPPE Require MPPE(40/128 bit) Maximum MPPE(128 bit) Maximum MPPE(128 bit) Coptional MPPE (40/128 bit) Maximum MPPE(128 bit) Maximum MPPE(128 bit) Require MPPE (40/128 bit) - Selecting this option will force the router to encrypt packets by using the MPPE encryption algorithm. In addition, the remote dial-in user will use 40-bit to perform encryption prior to using 128-bit for encryption. In other words, if 128-bit MPPE encryption method is not available, then 40-bit encryption scheme will be applied to encrypt the data. Maximum MPPE - This option indicates that the router will use the MPPE encryption scheme with maximum bits (128-bit) to encrypt the data.
Mutual Authentication (PAP)	The Mutual Authentication function is mainly used to communicate with other routers or clients who need bi-directional authentication in order to provide stronger security, for example, Cisco routers. So you should enable this function when your peer router requires mutual authentication. You should further specify the User Name and Password of the mutual authentication peer.
Start IP Address	Enter a start IP address for the dial-in PPP connection. You should choose an IP address from the local private network. For example, if the local private network is 192.168.1.0/255.255.255.0, you could choose 192.168.1.200 as the Start IP Address. But, you have to notice that the first two IP addresses of 192.168.1.200 and 192.168.1.201 are reserved for ISDN remote dial-in user.

3.8.3 IPSec General Setup

In IPSec General Setup, there are two major parts of configuration.

There are two phases of IPSec.

- Phase 1: negotiation of IKE parameters including encryption, hash, Diffie-Hellman parameter values, and lifetime to protect the following IKE exchange, authentication of both peers using either a Pre-Shared Key or Digital Signature (x.509). The peer that starts the negotiation proposes all its policies to the remote peer and then remote peer tries to find a highest-priority match with its policies. Eventually to set up a secure tunnel for IKE Phase 2.
- Phase 2: negotiation IPSec security methods including Authentication Header (AH) or Encapsulating Security Payload (ESP) for the following IKE exchange and mutual examination of the secure tunnel establishment.

There are two encapsulation methods used in IPSec, **Transport** and **Tunnel**. The **Transport** mode will add the AH/ESP payload and use original IP header to encapsulate the data payload only. It can just apply to local packet, e.g., L2TP over IPSec. The **Tunnel** mode will not only add the AH/ESP payload but also use a new IP header (Tunneled IP header) to encapsulate the whole original IP packet.

Authentication Header (AH) provides data authentication and integrity for IP packets passed between VPN peers. This is achieved by a keyed one-way hash function to the packet to create a message digest. This digest will be put in the AH and transmitted along with packets. On the receiving side, the peer will perform the same one-way hash on the packet and compare the value with the one in the AH it receives.

Encapsulating Security Payload (ESP) is a security protocol that provides data confidentiality and protection with optional authentication and replay detection service.

IKE Authentication Method			
Pre-Shared Key	••••		
Confirm Pre-Shared Key	••••		
IPSec Security Method			
Medium (AH)			
Data will be authentic, b	out will not be encrypted.		
	3DES AES		
Data will be encrypted a	and authentic.		
IKE Authentication Method	OKCancelThis usually applies to those are remote dial-in user or node (LAN-to-LAN) which uses dynamic IP address and IPSec-related VPN connections such as L2TP over IPSec and IPSec tunnel.Pre-Shared Key -Currently only support Pre-Shared Key authentication.Pre-Shared Key- Specify a key for IKE authentication Confirm Pre-Shared Key-Confirm the pre-shared key.		
IPSec Security Method	Medium - Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is		

VPN and Remote Access >> IPSec General Setup

active.

High - Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.

3.8.4 IPSec Peer Identity

To use digital certificate for peer authentication in either LAN-to-LAN connection or Remote User Dial-In connection, here you may edit a table of peer certificate for selection. As shown below, the router provides 32 entries of digital certificates for **peer users**.

		-			Factory Defau
Index	Name	Status	Index	Name	Status
<u>1.</u>	???	×	<u>17.</u>	???	×
<u>2.</u>	???	×	<u>18.</u>	???	×
<u>3.</u>	???	×	<u>19.</u>	???	×
<u>4.</u>	???	×	<u>20.</u>	???	×
<u>5.</u>	???	×	<u>21.</u>	???	Х
<u>6.</u>	???	×	<u>22.</u>	???	×
<u>7.</u>	???	×	<u>23.</u>	???	×
<u>8.</u>	???	×	<u>24.</u>	???	×
<u>9.</u>	???	×	<u>25.</u>	???	×
<u>10.</u>	???	×	<u>26.</u>	???	×
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	×	<u>28.</u>	???	×
<u>13.</u>	???	×	<u>29.</u>	???	Х
<u>14.</u>	???	×	<u>30.</u>	???	×
<u>15.</u>	???	×	<u>31.</u>	???	Х
<u>16.</u>	???	×	<u>32.</u>	???	×

VPN and Remote Access >> IPSec Peer Identity

Set to Factory Default

Click it to clear all indexes.

Index

Click the number below Index to access into the setting page of IPSec Peer Identity.

Name Display the profile name of that index.

Click each index to edit one peer digital certificate. There are three security levels of digital signature authentication: Fill each necessary field to authenticate the remote peer. The following explanation will guide you to fill all the necessary fields.

VPN	and	Remote	Access	>>	IPSec	Peer	Identity

Profile Name	one	
🗹 Enable this	account	
O Accept Any	Peer ID	
Accept Subj	ect Alternative Name	
Туре		IP Address 💌
IP		
🔿 Accept Subj	ect Name	
Country (C)		
State (ST)		
Location (L)		
Orginization (0)	
Orginization l	Jnit (OU)	
Common Nam	ie (CN)	
Email (E)		

Profile Name	Type in a name in this file.
Enable this account	Check this box to enable such profile.
Accept Any Peer ID	Click to accept any peer regardless of its identity.
Accept Subject Alternative Name	Click to check one specific field of digital signature to accept the peer with matching value. The field can be IP Address , Domain , or E-mail Address . The box under the Type will appear according to the type you select and ask you to fill in corresponding setting.
Accept Subject Name	Click to check the specific fields of digital signature to accept the peer with matching value. The field includes Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN), and Email (E).

3.8.5 Remote Dial-in User

You can manage remote access by maintaining a table of remote user profile, so that users can be authenticated to dial-in via ISDN or build the VPN connection. You may set parameters including specified connection peer ID, connection type (ISDN Dial-In connection, VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides 32 access accounts for dial-in users. Besides, you can extend the user accounts to the RADIUS server through the built-in RADIUS client function. The following figure shows the summary table.

emote Access	User Accounts:			Set to F	actory Defaul
Index	user	Status	Index	User	Status
<u>1.</u>	???	×	<u>17.</u>	???	Х
<u>2.</u>	777	×	<u>18.</u>	???	Х
<u>3.</u>	???	×	<u>19.</u>	???	X
<u>4.</u>	???	×	<u>20.</u>	???	×
<u>5.</u>	???	×	<u>21.</u>	???	X
<u>6.</u>	???	×	<u>22.</u>	???	X
<u>7.</u>	???	×	<u>23.</u>	???	Х
<u>8.</u>	???	×	<u>24.</u>	???	Х
<u>9.</u>	???	×	<u>25.</u>	???	X
<u>10.</u>	???	×	<u>26.</u>	???	Х
<u>11.</u>	???	×	<u>27.</u>	???	Х
<u>12.</u>	???	×	<u>28.</u>	???	×
<u>13.</u>	???	×	<u>29.</u>	???	X
<u>14.</u>	???	×	<u>30.</u>	???	×
<u>15.</u>	???	×	<u>31.</u>	???	X
<u>16.</u>	???	×	<u>32.</u>	???	X

VPN and Remote Access >> Remote Dial-in User

Set to Factory Default	Click to clear all indexes.	
Index	Click the number below Index to access into the setting page of Remote Dial-in User.	
User	Display the username for the specific dial-in user of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.	
Status	Display the access state of the specific dial-in user. The symbol V and X represent the specific dial-in user to be active and inactive, respectively.	
Click each index to edit one remote user profile Each Dial-In Type requires you to fill the		

Click each index to edit one remote user profile. **Each Dial-In Type requires you to fill the different corresponding fields on the right.** If the fields gray out, it means you may leave it untouched. The following explanation will guide you to fill all the necessary fields.

VPN and Remote Access >> Remote Dial-in User

Jser account and Authentication	
🗹 Enable this account	Username ???
Idle Timeout 300 second(s)	Password
Allowed Dial-In Type	IKE Authentication Method
ISDN	🗹 Pre-Shared Key
PPTP	IKE Pre-Shared Key
🗹 IPSec Tunnel	Digital Signature (X.509)
🗹 L2TP with IPSec Policy None 💌	None 💌
Specify Remote Node Remote Client IP or Peer ISDN Number	IPSec Security Method
	Medium (AH)
	High (ESP)
or Peer ID	🗹 DES 🗹 3DES 🗹 AES
	Local ID (optional)
	Callback Function
	Check to enable Callback function
	Specify the callback number
	Callback Number
	Check to enable Callback Budget Control
	Callback Budget 30 minute(s)

Clear

Cancel

Enable this account Check the box to enable this function. Idle Timeout- If the dial-in user is idle over the limitation of the timer, the router will drop this connection. By default, the Idle Timeout is set to 300 seconds. **ISDN** Allow the remote ISDN dial-in connection. You can further set up Callback function below. You should set the User Name and Password of remote dial-in user below. This feature is for *i* model only. **PPTP** Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below **IPSec Tunnel** Allow the remote dial-in user to make an IPSec VPN connection through Internet. L2TP Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None - Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have - Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must -Specify the IPSec policy to be definitely applied on the L2TP connection. **Specify Remote Node** Check the checkbox-You can specify the IP address of the remote dial-in user, ISDN number or peer ID (used in IKE aggressive mode). Uncheck the checkbox-This means the connection type you

	select above will apply the authentication methods and security methods in the general settings .
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	 d This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and select one predefined in the X.509 Peer ID Profiles (set from VPN and Remote Access>>IPSec Peer Identity)
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Check the Medium, DES, 3DES or AES box as the security method. Medium -Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is invoked. You can uncheck it to disable it. High-Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES. Local ID - Specify a local ID to be used for Dial-in setting in the LAN-to-LAN Profile setup. This item is optional and can be used only in IKE aggressive mode.
Callback Function	 The callback function provides a callback service only for the ISDN dial-in user (for <i>i</i> model only). The remote user will be charged the connection fee by the telecom. Check to enable Callback function-Enables the callback function. Specify the callback number-The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Check to enable callback budget control-By default, the callback function has a time restriction. Once the callback budget has been exhausted, the callback mechanism will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased automatically per callback connection.

3.8.6 LAN to LAN

Here you can manage LAN-to-LAN connections by maintaining a table of connection profiles. You may set parameters including specified connection direction (dial-in or dial-out), connection peer ID, connection type (ISDN connection, VPN connection - including PPTP, IPSec Tunnel, and L2TP by itself or over IPSec) and corresponding security methods, etc.

The router provides up to 32 profiles, which also means supporting 32 VPN tunnels simultaneously. The following figure shows the summary table.

Index	Name	Status	Index	Name	Status
<u>1.</u>	2.29	×	<u>17.</u>	???	×
<u>2.</u>	2.229	×	<u>18.</u>	???	×
<u>3.</u>	24	×	<u>19.</u>	???	×
<u>4.</u>	25	×	<u>20.</u>	???	×
<u>5.</u>	26	×	<u>21.</u>	???	×
<u>6.</u>	27	×	<u>22.</u>	???	×
<u>7.</u>	28	×	<u>23.</u>	???	×
<u>8.</u>	29	×	<u>24.</u>	???	×
<u>9.</u>	30	×	<u>25.</u>	???	×
<u>10.</u>	???	×	<u>26.</u>	???	×
<u>11.</u>	???	×	<u>27.</u>	???	×
<u>12.</u>	???	×	<u>28.</u>	???	×
<u>13.</u>	???	×	<u>29.</u>	???	×
<u>14.</u>	???	×	<u>30.</u>	???	×
<u>15.</u>	???	×	<u>31.</u>	???	×
<u>16.</u>	???	×	32.	???	×

VPN and Remote Access >> LAN to LAN

[XXXXXX:This Dial-Out Profile has already joined for VPN BACKUP Mechanism] [XXXXX:This Dial-Out Profile does not join for VPN TRUNK]

Set to Factory Default	Click to clear all indexes.
Name	Indicate the name of the LAN-to-LAN profile. The symbol ??? represents that the profile is empty.
Status	Indicate the status of individual profiles. The symbol V and X represent the profile to be active and inactive, respectively.

LAN-to-LAN profiles are suitable for dial-out usage. If the profile name displayed in red, it means that the profile has been grouped into VPN TRUNK. If the profile name displayed in black, it means that profile is not grouped into VPN TRUNK and can be invoked individually.

LAN-to-LAN Profiles:			
Index	Name	Status	
<u>1.</u>	2.5	V	
<u>2.</u>	2.5-1	V	
<u>3.</u>	2.29	V	
<u>4.</u>	2.229	V	
<u>5.</u>	26	V	
<u>6.</u>	27	V	
Ζ.	28	V	
<u>8.</u>	29	V	
<u>9.</u>	30	V	
10.	31	V	

Click each index to edit each profile and you will get the following page. Each LAN-to-LAN profile includes 4 subgroups. If the fields gray out, it means you may leave it untouched. The following explanations will guide you to fill all the necessary fields.

When VPN TRUNK is activated, several fields (e.g., Dial-in Settings, Dial-in selection in Call Direction and others) might be locked and dimmed. Please refer to **VPN and Remote Access>>VPN TRUNK Management** for more details.

Check here to activate this profile.

For the web page is too long, we divide the page into several sections for explanation.

Profile Index : 1 1. Common Settings Profile Name first Call Direction 💿 Both 🔘 Dial-Out 🔘 Dial-In Always on 🗹 Enable this profile Idle Timeout 300 second(s) VPN Connection Through: WAN1 First 💌 📃 Enable PING to keep alive PING to the IP 2. Dial-Out Settings Type of Server I am calling Link Type 64k bps 💌 ISDN Username 222 ○ РРТР Password IPSec Tunnel **PPP** Authentication PAP/CHAP 🔽 O L2TP with IPSec Policy None VJ Compression 💿 On 🔘 Off Dial Number for ISDN or IKE Authentication Method Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89) Pre-Shared Key 🔵 Digital Signature(X.509) **IPSec Security Method** Medium(AH) O High(ESP) DES without Authentication 📝 Advanced Index(1-15) in Schedule Setup: . Callback Function (CBCP) Require Remote to Callback Provide ISDN Number to Remote **Profile Name** Specify a name for the profile of the LAN-to-LAN connection.

Enable this profile

VPN Connection Through Use the drop down menu to choose a proper WAN interface for this profile. This setting is useful for dial-out only.

VPN Connection Through:

First	*
First	
Only	
First	
Only	
	First

	 WAN1 First - While connecting, the router will use WAN1 as the first channel for VPN connection. If WAN1 fails, the router will use another WAN interface instead. WAN1 Only - While connecting, the router will use WAN1 as the only channel for VPN connection. WAN2 First - While connecting, the router will use WAN2 as the first channel for VPN connection. If WAN2 fails, the router will use another WAN interface instead. WAN2 Only - While connecting, the router will use WAN2 as the only channel for VPN connection.
Call Direction	Specify the allowed call direction of this LAN-to-LAN profile. Both:-initiator/responder Dial-Out- initiator only Dial-In- responder only.
Always On or Idle Timeout	Always On-Check to enable router always keep VPN connection.Idle Timeout: The default value is 300 seconds. If the connection has been idled over the value, the router will drop the connection.
Enable PING to keep alive	This function is to help the router to determine the status of IPSec VPN connection, especially useful in the case of abnormal VPN IPSec tunnel disruption. For details, please refer to the note below. Check to enable the transmission of PING packets to a specified IP address.
PING to the IP	Enter the IP address of the remote host that located at the other-end of the VPN tunnel.
	Enable PING to Keep Alive is used to handle abnormal IPSec VPN connection disruption. It will help to provide the state of a VPN connection for router's judgment of redial. Normally, if any one of VPN peers wants to disconnect the connection, it should follow a serial of packet exchange procedure to inform each other. However, if the remote peer disconnect without notice, Vigor router will by no where to know this situation. To resolve this dilemma, by continuously sending PING packets to the remote host, the Vigor router can know the true existence of this VPN connection and react accordingly. This is independent of DPD (dead peer detection).
ISDN	If you want to connect two networks with ISDN connection, please select ISDN radio button to build ISDN dial-out connection to the server. You should set up Link Type and identity like User Name and Password for the authentication

	of remote server. You can further set up Callback (CBCP) function below. This feature is useful for <i>i</i> model only.
PPTP	Build a PPTP VPN connection to the server through the Internet. You should set the identity like User Name and Password below for the authentication of remote server.
IPSec Tunnel	Build an IPSec VPN connection to the server through Internet.
L2TP with	 Build a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None: Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have: Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-out VPN connection becomes one pure L2TP connection. Must: Specify the IPSec policy to be definitely applied on the L2TP connection.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
PPP Authentication	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. PAP/CHAP is the most common selection due to wild compatibility.
VJ compression	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. VJ Compression is used for TCP/IP protocol header compression. Normally set to Yes to improve bandwidth utilization.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy. Pre-Shared Key -Input 1-63 characters as pre-shared key. Digital Signature (X.509) – Click this radio button to invoke this function and select one predefined in the X.509 Peer ID Profiles (set from VPN and Remote Access>>IPSec Peer Identity).
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy.
Medium	Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active.
	 High (ESP-Encapsulating Security Payload)- means payload (data) will be encrypted and authenticated. Select from below: DES without Authentication -Use DES encryption algorithm and not apply any authentication scheme. DES with Authentication-Use DES encryption algorithm and apply MD5 or SHA-1 authentication algorithm. 3DES without Authentication-Use triple DES encryption algorithm and not apply any authentication scheme. 3DES with Authentication-Use triple DES encryption

algorithm and apply MD5 or SHA-1 authentication algorithm. **AES without Authentication**-Use AES encryption algorithm and not apply any authentication scheme. **AES with Authentication**-Use AES encryption algorithm and

apply MD5 or SHA-1 authentication algorithm.

Advanced

Specify mode, proposal and key life of each IKE phase, Gateway etc.

The window of advance setup is shown as below:

(<mark>ک</mark>	ttp://192.168.1.1 - IKE adva	nced settings - Microsoft Internet Explorer	
	KE advanced settings		
	IKE phase 1 mode	Main mode O Aggressive mode	
	IKE phase 1 proposal	DES_MD5_G1/DES_SHA1_G1/3DES_MD5_G1/3DES_MD5_G2/AES128_MD5_G2/AES256_SHA1_G2/AES256_SHA1_G14	•
	IKE phase 2 proposal	HMAC_SHA1/HMAC_MD5	
	IKE phase 1 key lifetime	28800 (900 ~ 86400)	
	IKE phase 2 key lifetime	3600 (600 ~ 86400)	
	Perfect Forward Secret	Disable O Enable	
	Local ID		
_		OK Close	

IKE phase 1 mode -Select from **Main** mode and **Aggressive** mode. The ultimate outcome is to exchange security proposals to create a protected secure channel. **Main** mode is more secure than **Aggressive** mode since more exchanges are done in a secure channel to set up the IPSec session. However, the **Aggressive** mode is faster. The default value in Vigor router is Main mode.

IKE phase 1 proposal-To propose the local available authentication schemes and encryption algorithms to the VPN peers, and get its feedback to find a match. Two combinations are available for **Aggressive** mode and thirty for **Main** mode. We suggest you select the combination that covers the most schemes. Below shows the available proposals:

DES MD5 G1
DES SHA1 G1
3DES MD5 G1
3DES SHAT G1
AES128 MD5 G1
AES128 SHAT G1
AES192 MD5 G1
AES192 SHAT G1
AES256 MD5 G1
AES256 SHAT G1
DES_MD5_G2
DES_SHA1_G2
3DES_MD5_G2
3DES_SHA1_G2
AES128_MD5_G2
AES128_SHA1_G2
AES192_MD5_G2
AES192_SHA1_G2
AES256_MD5_G2
AES256_SHA1_G2
DES_MD5_G14
DES_SHA1_G14
3DES_MD5_G14
3DES_SHA1_G14
AES128_MD5_G14
AES128_SHA1_G14
AES192_MD5_G14
AES192_SHA1_G14
AES256_MD5_G14
AES256_SHA1G14
AES256 SHA1 G14

IKE phase 2 proposal-To propose the local available algorithms to the VPN peers, and get its feedback to find a match. Three combinations are available for both modes. We suggest you select the combination that covers the most algorithms.

IKE phase 1 key lifetime-For security reason, the lifetime of key should be defined. The default value is 28800 seconds. You may specify a value in between 900 and 86400 seconds. **IKE phase 2 key lifetime-**For security reason, the lifetime of key should be defined. The default value is 3600 seconds. You may specify a value in between 600 and 86400 seconds. **Perfect Forward Secret (PFS)-**The IKE Phase 1 key will be reused to avoid the computation complexity in phase 2. The default value is inactive this function.

Local ID-In **Aggressive** mode, Local ID is on behalf of the IP address while identity authenticating with remote VPN server. The length of the ID is limited to 47 characters.

The callback function provides a callback service as a part of PPP suite only for the ISDN dial-in user. The router owner will be charged the connection fee by the telecom. **Require Remote to Callback-**Enable this to let the router to require the remote peer to callback for the connection afterwards.

Provide ISDN Number to Remote-In the case that the remote peer requires the Vigor router to callback, the local ISDN number will be provided to the remote peer. Check here to allow the Vigor router to send the ISDN number to the remote router. This feature is useful for *i* model only.

Callback Function (for *i* models only)

3	Dial	l In	Settings
э.	Dia	-111	Settings

Allowed Dial-In Type				
ISDN		Username	???	
PPTP		Password		
🗹 IPSec Tunnel		VJ Compression	💿 On 🔘 Off	
L2TP with IPSec Poli		IKE Authentication Methe	o d	
Peer ISDN Number or Pe	or Remote VPN Gateway	IKE Pre-Shared Key		
or Peer ID		Digital Signature(X.50	Digital Signature(X.509)	
		IPSec Security Method Medium (AH) High (ESP) DES 3DES Callback Function (CBCP Enable Callback Fun Use the Following N Callback Number Callback Budget	ction	
4. TCP/IP Network Settings	\$			
My WAN IP	0.0.0.0	RIP Direction	Disable 🍟	
Remote Gateway IP	0.0.0.0	From first subnet to ren do	note network, you have to	
Remote Network IP	0.0.0.0		Route 💌	
Remote Network Mask	255.255.255.0 More	Change default route to this VPN tunnel (Only single WAN supports this)		
	ОК	Clear Cancel		

Allowed Dial-In Type	Determine the dial-in connection with different types.
ISDN	Allow the remote ISDN LAN-to-LAN connection. You should set the User Name and Password of remote dial-in user below. This feature is useful for <i>i</i> model only. In addition, you can further set up Callback function below.
PPTP	Allow the remote dial-in user to make a PPTP VPN connection through the Internet. You should set the User Name and Password of remote dial-in user below.
IPSec Tunnel	Allow the remote dial-in user to trigger an IPSec VPN connection through Internet.
L2TP	 Allow the remote dial-in user to make a L2TP VPN connection through the Internet. You can select to use L2TP alone or with IPSec. Select from below: None- Do not apply the IPSec policy. Accordingly, the VPN connection employed the L2TP without IPSec policy can be viewed as one pure L2TP connection. Nice to Have- Apply the IPSec policy first, if it is applicable during negotiation. Otherwise, the dial-in VPN connection becomes one pure L2TP connection. Must- Specify the IPSec policy to be definitely applied on the L2TP connection.
Specify CLID or Remote	You can specify the IP address of the remote dial-in user or

VPN Gateway	peer ID (should be the same with the ID setting in dial-in type) by checking the box. Enter Peer ISDN number if you select ISDN above (This feature is useful for <i>i</i> model only.). Also, you should further specify the corresponding security methods on the right side.
	If you uncheck the checkbox, the connection type you select above will apply the authentication methods and security methods in the general settings.
User Name	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
Password	This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
VJ Compression	VJ Compression is used for TCP/IP protocol header compression. This field is applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above.
IKE Authentication Method	This group of fields is applicable for IPSec Tunnels and L2TP with IPSec Policy when you specify the IP address of the remote node. The only exception is Digital Signature (X.509) can be set when you select IPSec tunnel either with or without specify the IP address of the remote node. Pre-Shared Key - Check the box of Pre-Shared Key to invoke this function and type in the required characters (1-63) as the pre-shared key. Digital Signature (X.509) – Check the box of Digital Signature to invoke this function and select one predefined in the X.509 Peer ID Profiles (set from VPN and Remote Access>>IPSec Peer Identity).
IPSec Security Method	This group of fields is a must for IPSec Tunnels and L2TP with IPSec Policy when you specify the remote node. Medium- Authentication Header (AH) means data will be authenticated, but not be encrypted. By default, this option is active. High- Encapsulating Security Payload (ESP) means payload (data) will be encrypted and authenticated. You may select encryption algorithm from Data Encryption Standard (DES), Triple DES (3DES), and AES.
Callback Function	The callback function provides a callback service only for the ISDN LAN-to-LAN connection (this feature is useful for <i>i</i> model only). The remote user will be charged the connection fee by the telecom. Check to enable Callback function -Enables the callback function. Callback number -The option is for extra security. Once enabled, the router will ONLY call back to the specified Callback Number. Callback budget - By default, the callback function has limitation of callback period. Once the callback budget is exhausted, the function will be disabled automatically. Callback Budget (Unit: minutes)- Specify the time budget for the dial-in user. The budget will be decreased

	automatically per callback connection. The default value 0 means no limitation of callback period.
My WAN IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Gateway IP	This field is only applicable when you select ISDN, PPTP or L2TP with or without IPSec policy above. The default value is 0.0.0.0, which means the Vigor router will get a remote Gateway PPP IP address from the remote router during the IPCP negotiation phase. If the PPP IP address is fixed by remote side, specify the fixed IP address here. Do not change the default value if you do not select ISDN, PPTP or L2TP.
Remote Network IP/ Remote Network Mask	Add a static route to direct all traffic destined to this Remote Network IP Address/Remote Network Mask through the VPN connection. For IPSec, this is the destination clients IDs of phase 2 quick mode.
More	Add a static route to direct all traffic destined to more Remote Network IP Addresses/ Remote Network Mask through the VPN connection. This is usually used when you find there are several subnets behind the remote VPN router.
RIP Direction	The option specifies the direction of RIP (Routing Information Protocol) packets. You can enable/disable one of direction here. Herein, we provide four options: TX/RX Both, TX Only, RX Only, and Disable.
RIP Version	Select the RIP protocol version. Specify Ver. 2 for greatest compatibility.
From first subnet to remote network, you have to do	If the remote network only allows you to dial in with single IP, please choose NAT , otherwise choose Route .
Change default route to this VPN tunnel	Check this box to change the default route with this VPN tunnel. Be aware that this setting is available only for one WAN interface is enabled. It is not available when both WAN interfaces are enabled.

3.8.7 VPN TRUNK Management

VPN TRUNK Management is a backup mechanism to set multiple VPN tunnels for using as backup tunnel. It can assure the network connection would not be cut off due to network environment blocked by any reason.

Features of VPN TRUNK

- VPN TRUNK can judge abnormal situation for the environment of VPN server and correct it to complete the backup of VPN Tunnel in real-time.
- > VPN TRUNK is complaint with all WAN modes (single/multi)
- Dial-out connection types contain IPSec, PPTP, L2TP, L2TP over IPSec and ISDN (depends on hardware specification)
- > The web page is simple to understand and easy to configure
- Filly compliant with VPN Server LAN Sit Single/Multi Network
- Mail Alert support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Syslog support, please refer to System Maintenance >> SysLog / Mail Alert for detailed configuration
- Specific ERD (Environment Recovery Detection) mechanism which can be operated by using Telnet command

VPN TRUNK profile will be activated when initial connection of single VPN tunnel is off-line. Before setting VPN TRUNK backup profile, please configure at least two sets of LAN-to-LAN profiles (with fully configured dial-out settings) first, otherwise you will not have selections for grouping Member1 and Member2.

Note: [Active:N	01The LAN-	to-LAN Profile is disable or unde	er Dial-In(Call Direction) at present.
No. Status	-	Member1(Active)Type	Member2(Active)Type
, Status Profile Name Member1	• Enable	e C Disable	t you want.
Member2		choose the combination that	
Attribute Mode	Backup		
et to Factory 1	Default	Add Edit Click to clear all VPN	Delete N TRUNK profile.
)		The order of VPN TR	NNK profile

VPN and Remote Access >> VPN TRUNK Management

Status (on Backup Profile	"v" means such profile is enabled.
---------------------------	------------------------------------

field)	"x" means such profile is disabled.
Name (on Backup Profile field)	Display the name of VPN TRUNK profile.
Member1 (on Backup Profile field)	Display the dial-out profile selected from the Member1 drop down list below.
Active (on Backup Profile field)	"Yes" means normal condition. "No" means the state might be disabled or that profile currently is set with Dial-in mode (for call direction) in LAN-to-LAN.
Type (on Backup Profile field)	Display the connection type for that profile, such as IPSec, PPTP, L2TP, L2TP over IPSec (NICE), L2TP over IPSec(MUST) and so on.
Member2 (on Backup Profile field)	Display the dial-out profile selected from the Member2 drop down list below.
Status	After choosing one of the profile listed above, please click Enable to activate this profile. If you click Disable , the selected VPN TRUNK profile will not have any effect for VPN tunnel.
Profile Name	Type a name for VPN TRUNK profile. Each profile can group two VPN connections set in LAN-to-LAN. The saved VPN profiles in LAN-to-LAN will be shown on Member1 and Member2 fields.
Member 1/Member2	Display the selection for LAN-to-LAN dial-out profiles (configured in VPN and Remote Access >> LAN-to-LAN) for you to choose for grouping under certain VPN backup profile. <i>No</i> - Index number of LAN-to-LAN dial-out profile. <i>Name</i> - Profile name of AN-to-LAN dial-out profile. <i>Connection Type</i> - Connection type of AN-to-LAN dial-out profile. <i>VPN ServerIP (Private Network)</i> - VPN Server IP of LAN-to-LAN dial-out profiles.
Attribute Mode	Display available mode for you to choose. At present, only backup function is provided by this system. It is not necessary for you to choose attribute mode for your router.
Add	Add and save new profile to the backup profile list. The corresponding members (LAN-to-LAN profiles) grouped in such new VPN TRUNK profile will be locked. The profiles in LAN-to-LAN will be displayed in red.
Edit	Click this button to save the changes to the Status (Enable or Disable), profile name, member1 or member2.
Delete	Click this button to delete the selected VPN TRUNK profile. The corresponding members (LAN-to-LAN profiles) grouped in the deleted VPN TRUNK profile will be released and that profiles in LAN-to-LAN will be displayed in black.

Time for activating VPN TRUNK profile

VPN TRUNK backup will be activated automatically after the initial connection of single VPN Tunnel off-line. The content in Member1/2 within VPN TRUNK backup profile is similar to dial-out profile configured in LAN-to-LAN web page. VPN TRUNK backup profile will process and handle everything unless it is off-line once it is activated.

How can you set a VPN TRUNK profile?

- 1. Go to **VPN and Remote Access>>LAN-to-LAN**. Set two or more LAN-to-LAN profiles first.
- 2. Access into VPN and Remote Access>>VPN TRUNK Management.
- 3. Set one group of VPN TRUNK backup profile by choosing **Enable** radio button, type a name for such profile, choose one of the LAN-to-LAN profiles from Member1 drop down list, choose one of the LAN-to-LAN profiles from Member2 drop down list, last click **Add**.

ackup profile list		Set to Factory Defa
Note: [Active:	NO]The LAN-to-LAN Profile is disable or under Dial-	In(Call Direction) at present.
	VpnBackup 3(YES)IPSec	Member2(Active)Type 4(YES)L2TP over IPSec(MUST) 2(YES)PPTP
Status	© Enable ○ Disable	
Profile Name		
Member1	Please choose the combination that you w	vant.
Member2	Please choose the combination that you w. No. <name> <connection-type> <vpn< td=""><td>ant. ServerIP(Private Network)></td></vpn<></connection-type></name>	ant. ServerIP(Private Network)>
Attribute Mode	5 2.2 L2TP 192.1 6 27 IPSec 192.1	.68.2.2(192.168.26.0) .68.0.27(192.168.27.0)
	7 28 PPTP 192.1 8 29 L2TP over IPSec(NICE)192.1 9 30 L2TP over IPSec(NICE)192.1	

VPN and Remote Access >> VPN TRUNK Management

4. Index No.1 is the first VPN TRUNK backup profile. LAN-to-LAN profile of Index 3 is chosen as Member1; LAN-to-LAN profile of index 4 is chosen as Member2. At the same time, LAN-to-LAN profiles of 3 and 4 will be expressed in red to indicate that they are fixed.

Index	Name	Status
<u>1.</u>	2.5	V
<u>2.</u>	2.5-1	V
<u>3.</u>	2.29	V
<u>4.</u>	2.229	V
<u>5.</u>	26	V
<u>6.</u>	27	V
<u>7.</u>	28	V
<u>8.</u>	29	V
<u>9.</u>	30	V
10.	31	∇

LAN-to-LAN Profiles:

3.8.8 Connection Management

You can find the summary table of all VPN connections. You may disconnect any VPN connection by clicking **Drop** button. You may also aggressively Dial-out by using Dial-out Tool and clicking **Dial** button.

VPN	Туре	Remote	IP .	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime
					т.,	т.,	D.,	Dv	
Current Pa	ge: 1						Pa	ge No.	Go >>
VPN Conne	ection State	us							
		Backup Mode:				*	Dial	J	
		General Mode:				*	Dial		
Dial-out To	ol					Refre	sh Sec	onds :	10 🗸 Refresh

VPN and Remote Access >> Connection Management

xxxxxxxx : Data isn't encrypted.

General Mode

This filed displays the profile configured in LAN-to-LAN (with Index number and VPN Server IP address). The VPN connection built by General Mode does not support VPN backup function.

				Refresi
Genera	al Mode <mark>:</mark>	(28)	192.168.0.28	•
Backu	p Mode:	(28)	192.168.0.28	_
			192.168.0.29	
atue			192.168.0.30	
atus		(31)	192.168.0.31	
		(32)	192.168.0.32	
	_	(33)	192.168.0.33	
pe	Remot	(34)	192.168.0.34	
Tunnel		(35)	192.168.0.35	
A1 Auth	192.168	(36)	192.168.0.36	
TP		(37)	192.168.0.37	
A1 Auth	192.168	(38)	192.168.0.38	-

XXXXXXXXXX

Backup Mode

This filed displays the profile name saved in VPN TRUNK Management (with Index number and VPN Server IP address). The VPN connection built by Backup Mode supports VPN backup function.

Backu	p Mode	(VpnLB)	192.168.2.103		•
		(VpnLB)	192.168.2.103		
atus		(VpnLB)	92.168.2.203		
		(PptpLB)	192.168.2.5		
		(PptpLB)	192.168.2.5		
pe	Remo	(test) 192	.168.0.26		
	_	(test) 192	.168.0.27		
Tunnel HA1 Auth	192.16	2.103 19	2.168.1.0/24	51	3

Dial

Click this button to execute dial out function.

Refresh Seconds

Choose the time for refresh the dial information among 5, 10, and 30.

Refresh

Click this button to refresh the whole connection status.

Note: The status of LAN to LAN for ISDN is shown on the page of Online Status.

Online Status

System Status						Syste	m Uptime: 1:19:30
LAN Status		Primary DI	NS: 194.10	9.6.66	Se	condary DNS	: 168.95.1.1
IP Address	TX P	ackets	RX Pac	kets			
192.168.1.1	2945	;	2547				
WAN 1 Status							
Enable	Line	Name	Me	ode	Up Tir	ne	
Yes	Ethernet		St	atic IP	1:19:	23	
IP	GW IP	TX Packe	ts TX	(Rate	RX Pa	ickets	RX Rate
172.16.3.229	172,16.3,1	388	3		701		6
WAN 2 Status							
Enable	Line	Name	Me	ode	Up Tir	ne	
No	Ethernet			-	00:00	:00	
IP	GW IP	TX Packe	ts TX	(Rate	RX Pa	ickets	RX Rate
		0	0		0	I	0
ISDN Status				>>	Dial ISDN	>> Drop I	<u>B1 >> Drop B2</u>
Channel Active	e Connection	TX Pkts	TX Rate	RX Pkts	RX Rat	te Up Time	AOC
B1 Idle []	0	0	0	0	0:0:0	0
B2 Idle []	0	0	0	0	0:0:0	0
D DOWI	N						

3.9 Certificate Management

A digital certificate works as an electronic ID, which is issued by a certification authority (CA). It contains information such as your name, a serial number, expiration dates etc., and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Here Vigor router support digital certificates conforming to standard X.509.

Any entity wants to utilize digital certificates should first request a certificate issued by a CA server. It should also retrieve certificates of other trusted CA servers so it can authenticate the peer with certificates issued by those trusted CA servers.

Here you can manage generate and manage the local digital certificates, and set trusted CA certificates. Remember to adjust the time of Vigor router before using the certificate so that you can get the correct valid period of certificate.

Below shows the menu items for Certificate Management.

Certificate Management
Local Certificate
Trusted CA Certificate
Certificate Backup

3.9.1 Local Certificate

Certificate Management >> Local Certificate

Name	Name Subject		Modify
Local			View Delete
ENERATE	IPORT REFRESH		
			~
			~

Generate

Click this button to open Generate Certificate Request window.

Subject Alternative Name	
Туре	IP Address 🔽 💌
IP	
Subject Name	
Country (C)	
State (ST)	
Location (L)	
Orginization (O)	
Orginization Unit (OU)	
Common Name (CN)	
Email (E)	
Кеу Туре	RSA Y
Key Size	1024 Bit 🗸

Generate

Type in all the information that the window request. Then click **Generate** again.

Import	Click this button to import a saved file as the certification information.
Refresh	Click this button to refresh the information listed below.
View	Click this button to view the detailed settings for certificate request.

Certificate Management >> Local Certificate

After clicking **Generate**, the generated information will be displayed on the window below:



Certificate Management >> Local Certificate

X509 Local Certificate Configuration

3.9.2 Trusted CA Certificate

Trusted CA certificate lists three sets of trusted CA certificate.

Certificate Management	t >> T	Fruste d	CА	Certifica	te
------------------------	--------	----------	----	-----------	----

X509 Trusted CA Certificate Configuration

 	View Delete
 	View Delete
 	View Delete

To import a pre-saved trusted CA certificate, please click **IMPORT** to open the following window. Use **Browse...** to find out the saved text file. Then click Import. The one you imported will be listed on the Trusted CA Certificate window. Then click **Import** to use the pre-saved file.

Certificate Management >> Trusted CA Certificate

port X509 Trusted CA Certificate	
Select a trusted CA certificate file.	
Browse.,	
Click Import to upload the certification.	
Import Cancel	

For viewing each trusted CA certificate, click **View** to open the certificate detail information window. If you want to delete a CA certificate, choose the one and click **Delete** to remove all the certificate information.

🖹 Ceri	tificate Information - Microsoft Inter	net Explorer		×
				^
	Certifi	cate Detail Information		
	Certificate Name:	Trusted CA-1		
	Issuer:			
	Subject:			
	Subject Alternative Name:			
	Valid From:			
	Valid To:			
		Close		
				~

3.9.3 Certificate Backup

Local certificate and Trusted CA certificate for this router can be saved within one file. Please click **Backup** on the following screen to save them. If you want to set encryption password for these certificates, please type characters in both fields of **Encrypt password** and **Retype password**.

Certificate Management >> Certificate Backup					
Certificate Backup / Restoration					
Backup					
	Encrypt password:				
	Retype password:				
	Click Backup to download certificates to your local PC as a file.				
Restoration					
	Select a backup file to restore.				
	Browse.				
	Decrypt password:				
	Click Restore to upload the file.				

3.10 VoIP

Voice over IP network (VoIP) enables you to use your broadband Internet connection to make toll quality voice calls over the Internet.

There are many different call signaling protocols, methods by which VoIP devices can talk to each other. The most popular protocols are SIP, MGCP, Megaco and H.323. These protocols are not all compatible with each other (except via a soft-switch server).

The Vigor V models support the SIP protocol as this is an ideal and convenient deployment for the ITSP (Internet Telephony Service Provider) and softphone and is widely supported. SIP is an end-to-end, signaling protocol that establishes user presence and mobility in VoIP structure. Every one who wants to talk using his/her SIP Uniform Resource Identifier, "SIP Address". The standard format of SIP URI is

sip: user:password @ host: port

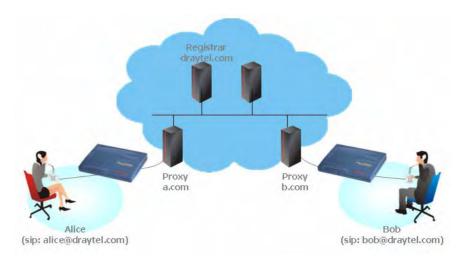
Some fields may be optional in different use. In general, "host" refers to a domain. The "userinfo" includes the user field, the password field and the @ sign following them. This is very similar to a URL so some may call it "SIP URL". SIP supports peer-to-peer direct calling and also calling via a SIP proxy server (a role similar to the gatekeeper in H.323 networks), while the MGCP protocol uses client-server architecture, the calling scenario being very similar to the current PSTN network.

After a call is setup, the voice streams transmit via RTP (Real-Time Transport Protocol). Different codecs (methods to compress and encode the voice) can be embedded into RTP packets. Vigor V models provide various codecs, including G.711 A/ μ -law, G.723, G.726 and G.729 A & B. Each codec uses a different bandwidth and hence provides different levels of voice quality. The more bandwidth a codec uses the better the voice quality, however the codec used must be appropriate for your Internet bandwidth.

Usually there will be two types of calling scenario, as illustrated below:

• Calling via SIP Servers

First, the Vigor V models of yours will have to register to a SIP Registrar by sending registration messages to validate. Then, both parties' SIP proxies will forward the sequence of messages to caller to establish the session.



If you both register to the same SIP Registrar, then it will be illustrated as below:

The major benefit of this mode is that you don't have to memorize your friend's IP address, which might change very frequently if it's dynamic. Instead of that, you will

only have to using **dial plan** or directly dial your friend's **account name** if you are with the same SIP Registrar. Please refer to the **section 4.5.1**.

Peer-to-Peer

Before calling, you have to know your friend's IP Address. The Vigor VoIP Routers will build connection between each other. Please refer to the **section 4.5.2**.



Our Vigor V models firstly apply efficient codecs designed to make the best use of available bandwidth, but Vigor V models also equip with automatic QoS assurance. QoS Assurance assists to assign high priority to voice traffic via Internet. You will always have the required inbound and outbound bandwidth that is prioritized exclusively for Voice traffic over Internet but you just get your data a little slower and it is tolerable for data traffic.



3.10.1 DialPlan

This page allows you to set phone book and digit map for the VoIP function. Click the **Phone Book** and **Digit Map** links on the page to access into next pages for dialplan settings.

VoIP >> DialPlan Setup

```
DialPlan Configuration

        Phone Book

        Digit Map
```

Phone Book

In this section, you can set your VoIP contacts in the "phonebook". It can help you to make calls quickly and easily by using "speed-dial" **Phone Number**. There are total 60 index entries in the phonebook for you to store all your friends and family members' SIP addresses. **Loop through** and **Backup Phone Number** will be displayed if you are using Vigor 2910VGi for setting the phone book.

VoIP >> DialPlan Setup

ndex	Phone number	Display Name	SIP URL	Loop through	Backup Phone Number	Status
<u>1.</u>	688	david	8201@iptel.org	None		v
<u>2.</u>				None		х
<u>3.</u>				None		х
<u>4.</u>				None		х
<u>5.</u>				None		х
<u>6.</u>				None		х
<u>7.</u>				None		х
<u>8.</u>				None		х
<u>9.</u>				None		х
<u>10.</u>				None		х
<u>11.</u>				None		х
<u>12.</u>				None		х
<u>13.</u>				None		х
<u>14.</u>				None		х
<u>15.</u>				None		х
<u>16.</u>				None		х
<u>17.</u>				None		х
<u>18.</u>				None		х
<u>19.</u>				None		х
<u>20.</u>				None		х
< 1-20	20-40 40-60	~~				<u>Next</u> >

Status: v --- Active, x --- Inactive, ? --- Empty

Click any index number to display the dial plan setup page.

```
VoIP >> DialPlan Setup
```

Phone Book Index No. 1	
🗹 Enable	
Phone Number	r 688
Display Name	david
SIP URL	8201 @ iptel.org
Enable Phone Number	OK Clear Cancel Click this to enable this entry. The speed-dial number of this index. This can be any number you choose, using digits 0-9 and * .
Display Name	The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.
SIP URL	Enter your friend's SIP Address

This page will differ for different models. Below is a sample page obtained from Vigor 2910VGi. The selection of **Loop through** and **Backup Phone Number** is only available for 2910VGi model.

VoIP >> DialPlan Se	tup				
Phone Book Index	No. 1				
🗹 Enable					
P	hone Number	1			
D	isplay Name	Polly			
s	IP URL	1112 @ fwd.pulver.com			
L	oop through	None 💌			
В	ackup Phone Nu	Imber			
	[OK Clear Cancel			
Enable		Click this to enable this entry.			
Phone Number	The speed-dial number of this index. This can be any numbry you choose, using digits 0-9 and *.				
Display Name		The Caller-ID that you want to be displayed on your friend's screen. This let your friend can easily know who's calling without memorizing lots of SIP URL Address.			
SIP URL		Enter your friend's SIP Address			
Loop through		For the model of Vigor 2910VGi, the selection should be as the following: Loop through			
Backup Phone Number		When the VoIP phone is obstructs or the Internet breaks down for some reasons, the backup phone will be dialed out to replace the VoIP phone number. At this time, the phone call will be changed from VoIP phone into PSTN call according to the loop through direction chosen. Note that, during the phone switch, the blare of phone will appear for a short time. And when the VoIP phone is switched into the PSTN phone, the telecom co. might charge you for the connection fee. Please type in backup phone number (PSTN number) for this VoIP phone setting.			

Digit Map

For the convenience of user, this page allows users to edit prefix number for the SIP account with adding number, stripping number or replacing number. It is used to help user having a quick and easy way to dial out through VoIP interface.

#	Enable	tup Prefix Number	Mod	e	OP Number	Min Len	Max Len	Interface
1		03	Replace	• •	8863	7	9	VolP1 💌
2		886	Strip	~	886	7	9	VolP1 💌
3			None	×		0	0	VolP1 👻
4			None	\sim		0	0	VolP1 👻
5			None	\vee		0	0	VolP1 🖌
6			None	\vee		0	0	VoIP1 💌
7			None	\vee		0	0	VolP1 👻
8			None	$\mathbf{\vee}$		0	0	VoIP1 💌
9			None	~		0	0	VolP1 💌
10			None	\vee		0	0	VoIP1 💌
11			None	\vee		0	0	VoIP1 💌
12			None	$\mathbf{\vee}$		0	0	VoIP1 💌
13			None	~		0	0	VolP1 👻
14			None	$\mathbf{\vee}$		0	0	VolP1 👻
15			None	Y		0	0	VolP1 💌
16			None	\mathbf{v}		0	0	VoIP1 👻
17			None	×		0	0	VolP1 👻
18			None	\mathbf{v}		0	0	VolP1 👻
19			None	×		0	0	VoIP1 👻
20			None	\sim		0	0	VolP1 🗸

OK]	Cancel

Enable Prefix Number	Check this box to invoke this setting. The phone number set here is used to add, strip, or replace the OP number.
Mode	 None - No action. Add - When you choose this mode, the OP number will be added with the prefix number for calling out through the specific VoIP interface. Strip - When you choose this mode, the OP number will be deleted by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886 will be deleted completely for the prefix number is set with 886. Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the OP number of 886. Replace - When you choose this mode, the OP number will be replaced by the prefix number for calling out through the specific VoIP interface. Take the above picture (Prefix Table Setup web page) as an example, the prefix number of 03 will be replaced by 8863. For example: dial number of "031111111" will be changed to "88631111111" and sent to

	SIP server. Mode Replace None Add Strip Replace
OP Number	The front number you type here is the first part of the account number that you want to execute special function (according to the chosen mode) by using the prefix number.
Min Len	Set the minimal length of the dial number for applying the prefix number settings. Take the above picture (Prefix Table Setup web page) as an example, if the dial number is between 7 and 9, that number can apply the prefix number settings here.
Max Len	Set the maximum length of the dail number for applying the prefix number settings.
Interface	Choose the one that you want to enable the prefix number settings from the saved SIP accounts. Please set up one SIP account first to make this interface available.

3.10.2 SIP Accounts

In this section, you set up your own SIP settings. When you apply for an account, your SIP service provider will give you an **Account Name** or user name, **SIP Registrar, Proxy,** and **Domain name**. (The last three might be the same in some case). Then you can tell your folks your SIP Address as in **Account Name@ Domain name**

As Vigor VoIP Router is turned on, it will first register with Registrar using AuthorizationUser@Domain/Realm. After that, your call will be bypassed by SIP Proxy to the destination using AccountName@Domain/Realm as identity.

Index	Profile	Domain/Realm	Proxy	Account Name	Ring Port	Status
1	david	iptel.org	iptel.org	8201	🗹 VoIP1 🗌 VoIP2 🗌 I	SDN -
<u>2</u>				change_me	🗌 VoIP1 🗌 VoIP2 🔲 I	SDN -
<u>3</u>				change_me	VoIP1 VoIP2 I	SDN -
<u>4</u>				change_me	🗌 VoIP1 🔲 VoIP2 🔲 I	SDN -
<u>5</u>				change_me	VoIP1 VoIP2 I	SDN -
<u>6</u>				change_me	VoIP1 VoIP2 I	SDN -
NAT Tra	versal Set	ting			 R: success registered c -: fail to register on SIP 	
	STUN	server:	stun.fv	vdnet.net		
	External IP:					
SIP PING interval:			150	sec		

VoIP >> SIP Accounts

Index

Click this link to access into next page for setting SIP account.

Profile	Display the profile name of the account.
Domain/Realm	Display the domain name or IP address of the SIP registrar server.
Proxy	Display the domain name or IP address of the SIP proxy server.
Account Name	Display the account name of SIP address before @.
Ring Port	Specify which port will ring when receiving a phone call.
STUN Server	Type in the IP address or domain of the STUN server.
External IP	Type in the gateway IP address.
SIP PING interval	The default value is 150sec. It is useful for a Nortel server NAT Traversal Support.
Status	Show the status for the corresponding SIP account. \mathbf{R} means such account is registered on SIP server successfully. – means the account is failed to register on SIP server.

VoIP >> SIP Accounts

Profile Name	test (11 char ma	x.)
Register via	None 💌 📃 make call withou	ut register
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
🗌 Act as outbound p	roxy	
Display Name	(23 char ma	x.)
Account Number/Name	8201	(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 💌 3600 sec	
NAT Traversal Support	None 💌	
Ring Port	VoIP1 VoIP2 ISDN	
Ring Pattern	1 🗸	

Profile NameAssign a name for this profile for identifying. You can type
similar name with the domain. For example, if the domain
name is *draytel.org*, then you might set *draytel-1* in this field.Register viaIf you want to make VoIP call without register personal
information, please choose None and check the box to achieve
the goal. Some SIP server allows user to use VoIP function
without registering. For such server, please check the box of
make call without register. Choosing Auto is recommended.

The system will select a proper way for your VoIP call.

Register via

None
None
Auto
WAN 1
WAN 2
LAN/VPN

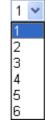
v

SIP Port	Set the port number for sending/receiving SIP message for building a session. The default value is 5060. Your peer must set the same value in his/her Registrar.				
Domain/Realm	Set the domain name or IP address of the SIP Registrar server. Set domain name or IP address of SIP proxy server. By the time you can type: port number after the domain name to specify that port as the destination of data transmission (e.g., nat.draytel.org: 5065)				
Proxy					
Act as Outbound Proxy	Check this box to make the proxy acting as outbound proxy.				
Display Name	The caller-ID that you want to be displayed on your friend's screen.				
Account Number/Name	Enter your account name of SIP Address, e.g. every text before @.				
Authentication ID	Check the box to invoke this function and enter the name or number used for SIP Authorization with SIP Registrar. If this setting value is the same as Account Name, it is not necessary for you to check the box and set any value in this field.				
Password	The password provided to you when you registered with a SIP service.				
Expiry Time	The time duration that your SIP Registrar server keeps your registration record. Before the time expires, the router will send another register request to SIP Registrar again.				
NAT Traversal Support	If the router (e.g., broadband router) you use connects to internet by other device, you have to set this function for your necessity.				
	NAT Traversal Support None None Stun manual nortel				
	 None – Disable this function. Stun – Choose this option if there is Stun server provided for your router. Manual – Choose this option if you want to specify an external IP address as the NAT transversal support. Nortel – If the soft-switch that you use supports nortel solution, you can choose this option. 				
Ring Port	Set VoIP1, VoIP 2 or ISDN as the default ring port for this SIP account. If you choose either VoIP1 or VoIP2, the ISDN selection will be dimmed, vice versa.				

Ring Pattern

Choose a ring tone type for the VoIP phone call.

Ring Pattern



Below shows successful SIP accounts for your reference.

VoIP >> SIP Accounts

index	Profile	Domain/Realm	Proxy	Account Name	F	ling Port		Statu
1	draytek_1	draytel.org	draytel.org	813177	🗹 VoIP1	VoIP2	ISDN	-
<u>2</u>	IPTEL	iptel.org	iptel.org	kevin_yu	VoIP1	VoIP2	I SDN	R
<u>3</u>	SeedNet	seednet.net.tw	139.175.232.13	070901002	🗌 VoIP1	🗹 VoIP2	ISDN	-
<u>4</u>				change_me	VoIP1	VoIP2	ISDN	-
<u>5</u>				change_me	VoIP1	VoIP2	🔲 ISDN	-
<u>6</u>				change_me	VoIP1	VoIP2	🗌 ISDN	-
IAT Tra	aversal Setti	ng				ss register register on		
	STUN s	erver:	stun.fwdr	iet.net				
	Externa	I IP:			7			
	SIP PIN	G interval:	150	sec	_			

3.10.3 Phone Settings

This page allows user to set phone settings for VoIP 1 and VoIP 2 respectively.

VoIP >> Phone Settings	VolP	>>	Phone	Settings
------------------------	------	----	-------	----------

Index	Port	Call feature	Codec	Tone	Gain (Mic/Speaker)	Default SIP Account	DTMF Relay	
1	FXS 1		G.729A/B	User Defined	5/5		InBand	
<u>2</u>	FXS 2		G.729A/B	User Defined	5/5		InBand	
<u>3</u>	ISDN		G.729A/B	User Defined	5/5		InBand	
RTP								
Symmetric RTP								
Dynamic RTP port start)050			
Dynamic RTP port end				15	5000			
RTP TOS				IF	precedence 5	▶ 1010000		

Phone List

Port – There are three phone ports provided here for you to configure.

Call feature – A brief description for call feature will be shown in this field for your reference.

Codec – The default Codec setting for each port will be

shown in this field for your reference. You can click the number below the Index field to change it for each phone port. **Tone** - Display the tone settings that configured in the advanced settings page of Phone Index.

Gain - Display the volume gain settings for Mic/Speaker that configured in the advanced settings page of Phone Index. **Default SIP Account** – "draytel_1" is the default SIP account. You can click the number below the Index field to change SIP account for each phone port.

DTMF Relay – Display DTMF mode that configured in the advanced settings page of Phone Index.

Symmetric RTP – Check this box to invoke the function. To make the data transmission going through on both ends of local router and remote router not misleading due to IP lost (for example, sending data from the public IP of remote router to the private IP of local router), you can check this box to solve this problem.

Dynamic RTP port start - Specifies the start port for RTP stream. The default value is 10050.

Dynamic RTP port end - Specifies the end port for RTP stream. The default value is 15000.

RTP TOS – It decides the level of VoIP package. Use the drop down list to choose any one of them.

Manual	
IP precedence 1	
IP precedence 2	
IP precedence 3	
IP precedence 4	
IP precedence 5	
IP precedence 6	
IP precedence 7	
AF Class1 (Low Drop)	
AF Class1 (Medium Drop)	
AF Class1 (High Drop)	
AF Class2 (Low Drop)	
AF Class2 (Medium Drop)	
AF Class2 (High Drop)	
AF Class3 (Low Drop)	
AF Class3 (Medium Drop)	
AF Class3 (High Drop)	
AF Class4 (Low Drop)	
AF Class4 (Medium Drop)	
AF Class4 (High Drop)	
EF Class	
Manual	~

RTP TOS

Detailed Settings for VoIP 1 and 2

Click the number 1 or 2 link under Index column, you can access into the following page for configuring Phone settings.

RTP

VoIP >> Phone Settings

Phone Index No.1			
Call feature		Codecs	
🔲 Hotline		Prefer Codec	G.729A/B (8Kbps) 🔽
Session Timer	3600 sec		Single Codec
T.38 Fax Function		Packet Size	20ms 🗙
		Voice Active Detector	Off 🖌
Call Forwarding	disable 💌		
SIP URL		Default SIP Account	1-??? 💙
Time Out	30 sec	Play dial tone only will	nen account registered
🔲 DND(Do Not Disturb) N	Mode	Default Call Route	
Index(1-15) in <u>Sche</u>	dule Setup:	◯ To ISDN: Dial *#	for VoIP
		⊙ To VoIP: Dial #	for ISDN
Note: Action and Idle Timeout settings will be ignored.			
Index(1-60) in <u>Phon</u>	e Book as Exception List:		
	,,,,		
🔲 CLIR (hide caller ID)			
🔲 Call Waiting			
🔲 Call Transfer			
	OK Car	ncel Advanced	

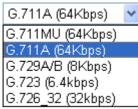
Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.		
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.		
T.38 Fax Function	If the remote end also supports FAX function, you can check this box to enable this function.		
Call Forwarding	There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means the incoming calls will be forwarded into SIP URL only when the local system is busy. No answer means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.		
	Call Forwarding disable always busy no answer SIP URL – Type in the SIP URL (e.g., aaa@draytel.org or abc@iptel.org) as the site for call forwarded. Time Out – Set the time out for the call forwarding. The		
DND (Do Not Disturb) mode	default setting is 30 sec. Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.		
	detailed configuration.		

profiles. Refer to section **3.10.1 DialPlan – Phone Book** for detailed configuration.

- **Call Waiting** Check this box to invoke this function. A notice sound will appear to tell the user new phone call is waiting for your response. Click hook flash to pick up the waiting phone call.
- Call TransferCheck this box to invoke this function. Click hook flash to
initiate another phone call. When the phone call connection
succeeds, hang up the phone. The other two sides can
communicate, then.

Prefer CodecSelect one of five codecs as the default for your VoIP calls.
The codec used for each call will be negotiated with the peer
party before each session, and so may not be your default
choice. The default codec is G.729A/B; it occupies little
bandwidth while maintaining good voice quality.
If your upstream speed is only 64Kbps, do not use G.711
codec. It is better for you to have at least 256Kbps upstream if
you would like to use G.711.

Prefer Codec



Single Codec – If the box is checked, only the selected Codec will be applied.

Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

Packet Size

20ms	*
10ms	
20ms	
30ms	
40ms	
50ms	
60ms	

Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Voice Active Detector



Default SIP AccountYou can set SIP accounts (up to six groups) on SIP Account
page. Use the drop down list to choose one of the profile
names for the accounts as the default one for this phone
setting.Play dial tone only when account registered - Check this
box to invoke the function.Default Call RouteIt determines the default direction for the call route of the
router.

To ISDN (for VoIP) - The router is set by using ISDN call.

To change ISDN call into VoIP call, please dial the character in this field for transferring. The character that you can type can be *, #, and $0 \sim 9$.

To VoIP (for ISDN) - The router is set by using VoIP call. To change VoIP call into ISDN call, please dial the character in this field for transferring. The character that you can type can be *, #, and $0 \sim 9$.

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

Tone Set	tings						
Region	UK	*		Ca	aller ID Type	FSK_ETSI (U	K) N
		Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dia	al tone	350	440	0	0	0	0
Ring	ing tone	400	450	400	200	400	2000
Bus	sy tone	400	0	375	375	0	0
Conge	stion tone	480	620	400	350	225	525
Volume (Gain			DTMF			
Mic Gain	(1-10)	5		DTMF mo	de	InBand	~
Speaker	Gain(1-10)	5		Payload 1	Type(rfc2833)	101	
MISC							
Dial Tone	e Power Leve	el 2	7				
Ring Free	quency	2	5				

VoIP >> Phone Settings

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

Tone Sett	ings		
Region	UK	*	
	User Defined		los
	UK		- (
Dia	US Denmark		0
Ringi	italy Germany		0
Bus	Netherlands		0
Conges	Portugal Sweden		0
Volume G	Australia		

Mic Gain(1-10)

Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.

Caller ID Type There are several standards provided here for displaying the caller ID on the panel of the telephone set. Choose the one that is suitable for the phone set according to the area of the router installed. If you don't know what standard that the phone set supports, please use the default setting.

Caller ID Type	FSK_ETSI	~
	FSK_ETSI FSK_ETSI (UK) FSK_BELLCORE (US/AU) DTMF DTMF	
200 375	DTMF (DK) DTMF (SE/NL/FIN) U	

Volume GainMic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of
microphone and speaker by entering number from 1-10. The
larger of the number, the louder the volume is.MISCDial Tone Power Level - This setting is used to adjust the
loudness of the dial tone. The smaller the number is, the

louder the dial tone is. It is recommended for you to use the default setting. **Ring Frequency** - This setting is used to drive the frequency

Ring Frequency - This setting is used to drive the frequency of the ring tone. It is recommended for you to use the default setting.

InBand - Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone **OutBand** - Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone.

SIP INFO- Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent

DTMF

to the remote end with SIP message.

InBand InBand OutBand (RFC2833) SIP INFO (cisco format) SIP INFO (nortel format)

Payload Type (rfc2833)

Choose a number from 96 to 127, the default value was 101. This setting is available for the OutBand (RFC2833) mode.

Detailed Settings for ISDN (available for VGi model only)

DTMF mode

Click the number **3** link under Index column, you can access into the following page for configuring Phone settings.

VoIP >> Phone Settings

ISDN			
Call feature		Codecs	
Hotline		Prefer Codec	G.729A/B (8Kbps) 🛛 🖌
			📃 Single Codec
Session Timer	3600 sec	Packet Size	20ms 🚩
Call Forwarding	disable 🔽	Voice Active Detector	Off 🗸
SIP URL		Default SIP Account	1-??? 🔽
Time Out	30 sec	Play dial tone only will	hen account registered
🔲 DND(Do Not Disturb)	Mode		-
Index(1-15) in Sch	edule Setup:	FXO feature	
		Enable ISDN to VoIP (On-Net) Calls
Note: Action and Id be ignored.	dle Timeout settings will	Enable VoIP to ISDN (Off-Net) Calls
-	e Book as Exception List:	ISDN Loop Through Ring P	ort
Index(1-00) in <u>Filo</u>	,,,,,,	Only when Router MSN m then this will take effect.	apping ring port is not set
🔲 CLIR (hide caller ID)		💿 Broadcast call 🔘 FX	S1 🔘 FXS2

Hotline	Check the box to enable it. Type in the SIP URL in the field for dialing automatically when you pick up the phone set.
Session Timer	Check the box to enable the function. In the limited time that you set in this field, if there is no response, the connecting call will be closed automatically.
ISDN Loop Through Ring Port	 Click the radio button to specify which port will ring if MSN mapping ring port (configured in ISDN>>General Setup) is not set properly. Broadcast call – Both FXS1 and FXS2 will ring. FXS 1- Such port will ring. FXS 2- Such port will ring.
Call Forwarding	There are four options for you to choose. Disable is to close call forwarding function. Always means all the incoming calls will be forwarded into SIP URL without any reason. Busy means the incoming calls will be forwarded into SIP URL only when the local system is busy. No answer means if the incoming calls do not receive any response, they will be forwarded to the SIP URL by the time out.

- U	_		
(all	Forv	ward	Ina
Can	1.01.1	vai u	uuq

disable 🛛 👻
disable
always
busy
no answer

	abc@iptel.org) as the site f	P URL (e.g., aaa@draytel.org or for call forwarded. out for the call forwarding. The	
DND (Do Not Disturb) mode	Set a period of peace time without disturbing by VoIP phone call. During the period, the one who dial in will listen busy tone, yet the local user will not listen any ring tone.		
	profiles to control the DNI preconfigured schedules. R detailed configuration. Index (1-60) in Phone Bo	 Enter the index of schedule D mode according to the Refer to section 3.5.2 Schedule for ok - Enter the index of phone book 5.10.1 DialPlan – Phone Book for 	
CLIR (hide caller ID)	Check this box to hide the phone set.	caller ID on the display panel of the	
Prefer Codec	Select one of five codecs as the default for your W The codec used for each call will be negotiated w party before each session, and so may not be your choice. The default codec is G.729A/B; it occupie bandwidth while maintaining good voice quality. If your upstream speed is only 64Kbps, do not use codec. It is better for you to have at least 256Kbp you would like to use G.711.		
	Prefer Codec	G.711A (64Kbps) 🛛 🔽	
		G.711MU (64Kbps) G.711A (64Kbps)	
		G.729A/B (8Kbps)	
		G.723 (6.4kbps)	
		G.726_32 (32kbps)	
	Single Codec – If the box	is checked only the selected Codec	

Single Codec – If the box is checked, only the selected Codec will be applied.

Packet Size-The amount of data contained in a single packet. The default value is 20 ms, which means the data packet will contain 20 ms voice information.

Packet Size

20ms 🚩
10ms
20ms
30ms
40ms
50ms
60ms

Voice Active Detector - This function can detect if the voice on both sides is active or not. If not, the router will do something to save the bandwidth for other using. Click On to invoke this function; click off to close the function.

Off	×
Off	
On	

Default SIP Account	You can set SIP accounts (up to six groups) on SIP Account page. Use the drop down list to choose one of the profile names for the accounts as the default one for this phone setting.
Play dial tone only when account registered	Check this box to invoke the function.
FXO Feature	 Enable ISDN to VoIP (On-Net) Calls – Check this box to make all the outgoing calls from ISDN line to be forwarded to receivers by Internet. Enable VoIP to ISDN (Off-Net) Calls –Check this box to make all the incoming calls coming from Internet to be forwarded to receivers by ISDN line.

Voice Active Detector

In addition, you can press the **Advanced** button to configure tone settings, volume gain, MISC and DTMF mode. **Advanced** setting is provided for fitting the telecommunication custom for the local area of the router installed. Wrong tone settings might cause inconvenience for users. To set the sound pattern of the phone set, simply choose a proper region to let the system find out the preset tone settings and caller ID type automatically. Or you can adjust tone settings manually if you choose User Defined. TOn1, TOff1, TOn2 and TOff2 mean the cadence of the tone pattern. TOn1 and TOn2 represent sound-on; TOff1 and TOff2 represent the sound-off.

Tone Settings						
Region User Defined	*					
	Low Freq (Hz)	High Freq (Hz)	T on 1 (msec)	T off 1 (msec)	T on 2 (msec)	T off 2 (msec)
Dial tone	350	440	0	0	0	0
Ringing tone	400	450	400	200	400	2000
Busy tone	400	0	375	375	0	0
Congestion tone	0	0	0	0	0	0
Volume Gain			DTMF			
Mic Gain(1-10) 5			DTMF mode		InBand 😽 🌱	
Speaker Gain(1-10)	5		Payload Type(rfc2833) 101			
MISC						
Dial Tone Power Leve	1 2	7				
Authentication PIN Code Disallow VoIP to ISDN Calls with the Following Prefixes						
🔲 Check for ISDN to						
🔲 Check for VoIP to	ISDN Calls 🛛	000				

VoIP >> Phone Settings

Region

Select the proper region which you are located. The common settings of **Caller ID Type**, **Dial tone**, **Ringing tone**, **Busy tone** and **Congestion tone** will be shown automatically on the page. If you cannot find out a suitable one, please choose **User Defined** and fill out the corresponding values for dial tone, ringing tone, busy tone, congestion tone by yourself for VoIP phone.

	Advance Settings >> ISDN
	Tone Settings
	Region User Defined V User Defined OW UK
	Dia US Denmark 0 Ringi Italy 0 Germany Bus Netherlands 0
	Conges Portugal Sweden Volume GAustralia Mic Gain(Slovenia Czech Speaker (Slovakia
	Also, you can specify each field for your necessity. It is recommended for you to use the default settings for VoIP communication.
Volume Gain	Mic Gain (1-10)/Speaker Gain (1-10) - Adjust the volume of microphone and speaker by entering number from 1- 10. The larger of the number, the louder the volume is.
MISC	Dial Tone Power Level - This setting is used to adjust the loudness of the dial tone. The smaller the number is, the louder the dial tone is. It is recommended for you to use the default setting.
Authentication PIN Code	 Check for ISDN to VoIP Calls – Set a pin code for the router to authenticate which one is allowed to dial ISDN to VoIP call. The figure that you can type in this field is limited from three to eight with digits from zero to nine. Check for VoIP to ISDN Calls - Set a pin code for the router to authenticate which one is allowed to dial VoIP to ISDN call. The figure that you can type in this field is limited from three to eight with digits from zero to nine.
DTMP	 DTMF mode – There are four selections provided here: InBand:Choose this one then the Vigor will send the DTMF tone as audio directly when you press the keypad on the phone OutBand: Choose this one then the Vigor will capture the keypad number you pressed and transform it to digital form then send to the other side; the receiver will generate the tone according to the digital form it receive. This function is very useful when the network traffic congestion occurs and it still can remain the accuracy of DTMF tone. SIP INFO: Choose this one then the Vigor will capture the DTMF tone and transfer it into SIP form. Then it will be sent to the remote end with SIP message.

	DTMF mode	InBand	~	
		InBand OutBand (RFC2833)		
		SIP INFO (cisco format) SIP INFO (nortel format)		
	Payload Type (rfc2833) - (the default value was 101. T OutBand (RFC2833) mode.	This setting is available for		
Disallow VoIP to ISDN Calls with the Following Prefixes	Set the prefix of the phone r through VoIP to ISDN. All prefix specified here will no the router. If a user dials the disconnect it automatically. this field is limited one to el	the phone number with th of be allowed to connect the number by force, the rou The figure that you can ty	e nrou iter ype	ugh will in

3.10.4 Status

On VoIP call status, you can find codec, connection and other important call status for VoIP 1/2 ports.

VoIP >> Status

Status							F	Refresh Si	econds:	10 🗸	Refresh
Port	Status	Codec	PeerID	Elapse (hh:mm:ss)	Tx Pkts	Rx Pkts	Rx Losts	Rx Jitter (ms)	In Calls	Out Calls	Speaker Gain
VoIP1	IDLE			00:00:00	0	0	0	0	0	0	5
VoIP2	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN1	IDLE			00:00:00	0	0	0	0	0	0	5
ISDN2	IDLE			00:00:00	0	0	0	0	0	0	5

nine.

Date		Time	Duration	In/Out	Peer ID
(mm-dd-)	уууу)	(hh:mm:ss)	(hh:mm:ss)		
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	
00-00-	0	00:00:00	00:00:00	-	

Refresh Seconds

Specify the interval of refresh time to obtain the latest VoIP calling information. The information will update immediately when the Refresh button is clicked.

Refresh Seconds : 10 🚩



Port

It shows current connection status for the port of VoIP1, VoIP2, ISDN1 and ISDN2. The ISDN1/2 appears only when the router is equipped with ISDN interface. ISDN1 means B1 channel for the physical ISDN port; ISDN2 means B2 channel for the physical ISDN port. Be aware that ISDN1/2 port is available for the users living in Europe and using Vigor

	2910VGi only. For other V models, only the status for VoIP1 and VoIP2 will be shown in this page.
Status	It shows the VoIP connection status. IDLE - Indicates that the VoIP function is idle. HANG_UP - Indicates that the connection is not established (busy tone). CONNECTING - Indicates that the user is calling out. WAIT_ANS - Indicates that a connection is launched and waiting for remote user's answer. ALERTING - Indicates that a call is coming. ACTIVE-Indicates that the VoIP connection is launched.
Codec	Indicates the voice codec employed by present channel.
PeerID	The present in-call or out-call peer ID (the format may be IP or Domain).
Connect Time	The format is represented as seconds.
Tx Pkts	Total number of transmitted voice packets during this connection session.
Rx Pkts	Total number of received voice packets during this connection session.
Rx Losts	Total number of lost packets during this connection session.
Rx Jitter	The jitter of received voice packets.
In Calls	The accumulating in-call times.
Out Calls	The accumulating out-call times.
Speaker Gain	The volume of present call.
Log	Display logs of VoIP calls.

3.11 ISDN

ISDN means integrated services digital network that is an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires.

Below shows the menu items of ISDN for *i* models.



3.11.1 General Setup

This page provides some basic ISDN settings such as enabling the ISDN port or not, MSN numbers and blocked MSN numbers, etc.

ISDN >> General Setup

ISDN Setup			
ISDN Port	💿 Enable 🔘 Disable	Blocked MSN numbers for the router	
Country Code	International 🛛 👻	1	
Own Number		2.	
"Own Number" means that the router will tell the		з.	
remote end the ISDN number when it's placing an outgoing call.		4.	
		5.	
Index MSN numbe	rs for the router	Mapping to VoIP Ports:	
1.		FXS1 FXS2	
2.		FXS1 FXS2	
з.		FXS1 FXS2	
"MSN Numbers" means that the router is able to accept number-matched incoming calls. In addition, MSN service should be supported by the local ISDN network provider.			

Cancel

0K

ISDN Port Click Enable to open the ISDN port and Disable to close it. **Country Code** For proper operation on your local ISDN network, you should choose the correct country code. **Own Number** Enter your ISDN number. Every outgoing call will carry the number to the receiver. **Blocked MSN Numbers for the** Enter the specified MSN number into the fields to prevent the router from dialing the specific MSN router number. **MSN Numbers for the Router** MSN Numbers mean that the router is able to accept only number-matched incoming calls. In addition, MSN services should be supported by local ISDN network provider. The router provides three fields for MSN numbers. Note that MSN services must be acquired from your local telecommunication operators. By default, MSN function is disabled. If you leave the fields blank, all incoming calls will be accepted without number matching. **Mapping to VoIP Ports** Check to specify ringing from FXS1 and/or FXS2 when the router accepts the incoming calls by identifying MSN number(s). If you do not specify any port in this field, the ISDN loop through ring port will be determined by the configuration in ISDN port in VoIP>>Phone Settings.

3.11.2 Dialing to a Single ISP

If you access the Internet via a single ISP, press this link.

ISDN >> Dialing to a Single ISP	

Single ISP			
ISP Access Setup		PPP/MP Setup	
ISP Name	prima	Link Type	Dialup BOD 🛛 👻
Dial Number	9834737	PPP Authentication	PAP or CHAP
Username	amor	Idle Timeout IP Address Assignmer	180 second(s)
Password	•••••	Fixed IP	○ Yes ⊙ No (Dynamic IP)
Require ISP callbac	ck (CBCP)	Fixed IP Address	
Index(1-15) in <u>Sched</u>	<u>ule</u> Setup:		
=>,	,,		
		ок	

ISP Name	Enter your ISP name.
Dial Number	Enter the ISDN access number provided by your ISP.
Username	Enter the username provided by your ISP.
Password	Enter the password provided by your ISP.
Require ISP Callback (CBCP)	If your ISP supports the callback function, check this box to activate the Callback Control Protocol during the PPP negotiation.
Scheduler (1-15)	Enter the index of schedule profiles to control the Internet access according to the preconfigured schedules.
Link Type	There are four link types: Link Disable, Dialup 64 Kbps, Dialup 128 Kbps, and Dialup BOD. Link Disable - Disable the ISDN dial-out function. Dialup 64Kbps - Use one ISDN B channel for Internet access. Dialup 128Kbps - Use both ISDN B channels for Internet access. Dialup BOD - BOD stands for bandwidth-on-demand. The router will use only one B channel in low traffic situations. Once the single B channel bandwidth is fully used, the other B channel will be activated automatically through the dialup. For more detailed BOD parameter settings, please refer to the Advanced Setup field > Call Control and PPP/MP Setup.
PPP Authentication	PAP Only - Configure the PPP session to use the PAP protocol to negotiate the username and password with the ISP.PAP or CHAP - Configure the PPP session to use the PAP or CHAP protocols to negotiate the username and password with the ISP.
Idle Timeout	Idle timeout means the router will be disconnect after being idle for a preset amount of time. The default is 180 seconds. If you set the time to 0, the ISDN connection to the ISP will always remain on.
Fixed IP	In most environments, you should not change these settings as most ISPs provide a dynamic IP address for the router when it connects to the ISP. If your ISP provides a fixed IP address, check

Yes to invoke this function and enter the IP address in the field of Fixed IP Address.

Fixed IP Address Type the IP address.

3.11.3 Dialing to Dual ISPs

If you have more than one ISP, press this link to configure two ISP dialup profiles. You will be able to dial to both ISPs at the same time. This is mainly for those ISPs that do not support Multiple-Link PPP (ML-PPP) function. In such cases, dialing to two ISPs can increase the bandwidth utilization of the ISDN channels to 128kbps data speed.

ISDN >> Dialing to Dual ISPs

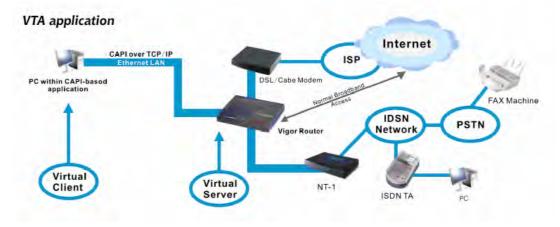
Common Settings		PPP/MP Setup		
1. 🗹 Enable Dual ISPs Function		Link Type	Dialup BOD 🛛 🔽	
2. 🔲 Require ISP (callback (CBCP)	PPP Authentication	PAP or CHAP 🔽	
		Idle Timeout	180 second(s)	
Primary ISP Setup		Secondary ISP Setu	0	
ISP Name	prima	ISP Name	dingo	
Dial Number	9834737	Dial Number	8849343	
Jsername	amor	Username	amor	
Password	•••••	Password	••••	
IP Address Assignm	ent Method (IPCP)	IP Address Assignment Method (IPCP)		
Fixed IP	🔘 Yes 💿 No (Dynamic IP)	Fixed IP	🔘 Yes 💿 No (Dynamic IP)	
Fixed IP Address		Fixed IP Address		

Most configuration parameters are the same as those of the previous part. This screen provides a checkbox to enable the Dual ISPs function and adds the secondary ISP Setup section field. Check the corresponding box and enter the second ISP information. About the details please refer to the descriptions of the previous part.

3.11.4 Virtual TA

Virtual TA means the local hosts or PCs in the network that uses popular CAPI-based software such as RVS-COM or BVRP to access the router as a local ISDN TA for sending or receiving FAX messages over the ISDN line. Basically, it is a client/server network model. The built-in Virtual TA server handles the establishment and release of connections. The Virtual TA client, which is installed on the local hosts or PCs, creates a CAPI-based driver to relay all CAPI messages between the applications and the router CAPI module. Before describing the configuration of **Virtual TA** in the Vigor routers, please notice the following limitations.

- The Virtual TA client only supports MicrosoftTM Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also two.
- Before you configure the Virtual TA, you must set the correct country code.



As depicted in the above application scenario, the Virtual TA client can make an outgoing call or accept an incoming call to/from a peer FAX machine or ISDN TA, etc.

Before describing the configuration of Virtual TA in the Vigor routers, please heed the following limitations.

- The Virtual TA client only supports MicrosoftTM Windows 98/SE/2000/XP platforms.
- The Virtual TA client only supports the CAPI 2.0 protocol and has no built-in FAX engine.
- One ISDN BRI interface has two B channels. The maximum number of active clients is also 2.
- Before you configure the Virtual TA, you must set the correct country code in **ISDN Setup**.

ISDN >> Virtual TA

		-	
Virtual	TA	Setu	р

Virtual TA	TA Server : 💿 Enable 🔘 Disable					
Virtual TA	Users Profiles	\$				
Usei	name	Password	MSN1	MSN2	MSN3	Active
1.						
2.						
3.						
4.						
5.						

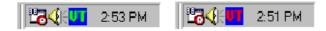
OK

 Virtual TA Server
 Enable: Select it to activate the server. Disable: Select it to deactivate the server. All Virtual TA applications will be terminated.
 Virtual TA User Profiles
 Username - Enter the username of a specific client. Password - Enter the password of a specific client. MSN 1/2/3 - MSN stands for Multiple Subscriber Number. It means you can apply to more than one ISDN lines number over a single subscribed line. Note that the service must be acquired from your telecom. Specify the MSN numbers for a specific client. If you have no MSN services, leave this field blank. Active - Check it to enable the client to access the server.

Install a Virtual TA Client

- 1. Insert the CD-ROM bundled with your Vigor router. Find **VTA Client** tool in the Utility menu and click on the Install button.
- 2. Follow the on-screen instructions of the installer. The last step will ask you to restart your computer. Click **OK** to restart your computer.
- 3. After the computer restarts, you will see a VT icon in the taskbar (usually in the bottom-right of the screen, near the clock) as shown below.

When the icon text is GREEN, the Virtual TA client is connected to the Virtual TA server and you can launch your CAPI-based software to use the client to access the router. If the icon text is RED, it means the client has lost the connection to the server. This time, please check the physical Ethernet connection.



Configure a Virtual TA Client/ Server

Since the Virtual TA application is a client/server network model, you must configure it on both ends to run properly your Virtual TA application.

By default, the Virtual TA server is enabled and the Username/Password fields are left blank. Any Virtual TA client may login to the server. Once a single Username/Password field has been filled in, the Virtual TA server will only allow clients with a valid Username/Password to login. The screen of Virtual TA configuration is presented below.

User Profile

Note that creating a single user access account will limit the access to the Virtual TA server to only the specified account holders.

Assume you did not acquire any MSN service from your ISDN network provider.

On the server - Click **Virtual TA (Remote CAPI) Setup** link, and fill in the Username and Password fields. Check the **Active** box to enable the account.

Vi	rtua	II TA Users Profile	s				
		Username	Password	MSN1	MSN2	MSN3	Active
	1.	alan	••••				
	2.						

On the client - Right-click the mouse on the VT icon. The following pop-up menu will be shown.

<u>A</u> uto Run <u>N</u> onauto Run	
<u>V</u> irtual TA Login	
<u>S</u> earch Server	
E <u>x</u> it	
	.

Click the Virtual TA Login tab to launch the login box.

Virtual TA Login	
User Name :	alan
Password :	****
OK DK	Cancel

Enter the Username/Password and then click **OK**. After a short time, the VT icon text will turn green.

MSN Configuration

If you have applied to an MSN number service, the Virtual TA server can assign which client has the specified MSN number. When an incoming call arrives, the server will inform the appropriate client. Now we set an example to describe the configuration of the MSN number.

Suppose that you could assign the MSN number 123 to the client "alan".

/irtual [·]	TA Users Profiles					
U	lsername	Password	MSN1	MSN2	MSN3	Active
1. al	lan	••••	123			~
2.						

Type the specified MSN number in the CAPI-based software. When the Virtual TA server sends an alert signal to the specified Virtual TA client, the CAPI-based software will also receive the action, the software will not accept the incoming call.

3.11.5 Call Control

Some applications require that the router (only for the ISDN models) be remotely activated, or be able to dial up to the ISP via the ISDN interface. Vigor routers provide this feature by allowing user to make a phone call to the router and then ask it to dial up to the ISP. Accordingly, a teleworker can access the remote network to retrieve resources. Of course, a fixed IP address is required for WAN connection and some internal network resource has to be exposed for remote users, such as FTP, WWW.Please set **Dialing to a Single ISP** first before configuring this web page.

ISDN >> Call Control

Call Control Setup		
Dial Retry	0 times	Remote Activation 1.
Dial Delay Interval	0 second(s)	2.
		3.
		4.
		5.

PPP/MP Dial-Out Setup

Basic Setup		Bandwidth On Demand (BOD) S	etup
Link Type	Dialup BOD 🛛 🖌	High Water Mark	7000 cps
PPP Authentication	PAP or CHAP 🖌	High Water Time	30 second(s)
TCP Header Compression	None 💌	Low Water Mark	6000 cps
Idle Timeout	180 second(s)	Low Water Time	30 second(s)



Dial Retry	It specifies the dial retry counts per triggered packet. A triggered packet is the packet whose destination is outside the local network. The default setting is no dial retry. If set to 5, for each triggered packet, the router will dial 5 times until it is connected to the ISP or remote access router.		
Dial Delay Interval	It specifies the interval between dialup retries. By default, the interval is 0 second.		
Remote Activation	It specifies a phone number in the Remote Activation field to enable the remote activation function. If the router accepts a call from the number 12345678, it will terminate the incoming call immediately and dial to the ISP.		
Link Type	Because ISDN has two B channels (64Kbps/per channel), you can specify whether you would like to have single B channel, two B channels or BOD (Bandwidth on Demand). Four options are available: Link Disable, Dialup 64Kbps, Dialup 128Kbps, Dialup BOD.		
	Link Type	Dialup BOD Link Disable Dialup 64Kbps Dialup 128Kbps Dialup BOD	

PPP Authentication	It specifies the PPP authentication method for PPP/MP connections. Normally you can set it to PAP/CHAP for better compatibility.			
TCP Header Compression	VJ Compression - It is used for TCP/IP protocol header compression. Normally it is set to None to improve bandwidth utilization.			
	TCP Header Compression None None None VJ COMP			
Idle Timeout	Because our ISDN link type is "Dial On Demand", the connection will be initiated only when needed.			
High Water Mark and High Water Time	BOD stands for bandwidth-on-demand for Multiple-Link PPP (ML-PPP or MP). High Water Mark/ High Water Time/ Low Water Mark/Low Water Time parameters are applied when you set the Link Type to Dialup BOD . The ISDN usually uses one B channel to access the Internet or remote network when you choose the Dialup BOD link type. The router will use the parameters here to decide on when you activate/drop the additional B channel. Note that cps (characters-per-second) measures the total link utilization.			
	These parameters specify the situation in which the second channel will be activated. With the first connected channel, if its utilization exceeds the High Water Mark and such a channel is being used over the High Water Time, the additional channel will be activated. Thus, the total link speed will be 128kbps (two B channels).			
Low Water Mark and Low Water Time	W These parameters specify the situation in which the second channel will be dropped. In terms of the two B channels, if their utilization is under the Low Water Mark and these two channels are being used over the High Water Time, the additional channel will be dropped. As a result, the total link speed will be 64kbps (one B channel).			
Note: If you are not sure whether your ISP can support BOD and/or ML-PPP's features, please seek assistance from your ISP, local dealers or our website: support@draytek.com .				

3.12 Wireless LAN

This function is used for G models only.

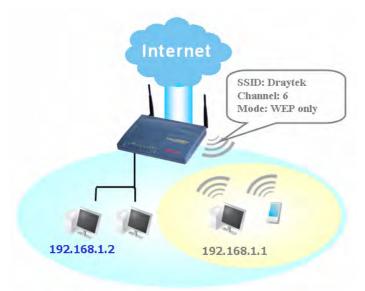
3.12.1 Basic Concepts

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the surface of the earth. Hundreds of millions of people exchange information every day via wireless communication products. The Vigor G model, a.k.a. Vigor wireless router, is designed for maximum flexibility and efficiency of a small office/home. Any authorized staff can bring a built-in WLAN client PDA or notebook into a meeting room for conference without laying a clot of LAN cable or drilling holes everywhere. Wireless LAN enables high mobility so WLAN users can simultaneously access all LAN facilities just like on a wired LAN as well as Internet access.

The Vigor wireless routers are equipped with a wireless LAN interface compliant with the standard IEEE 802.11g protocol. To boost its performance further, the Vigor Router is also loaded with advanced wireless technology Super GTM to lift up data rate up to 108 Mbps*. Hence, you can finally smoothly enjoy stream music and video.

Note: * The actual data throughput will vary according to the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.

In an Infrastructure Mode of wireless network, Vigor wireless router plays a role as an Access Point (AP) connecting to lots of wireless clients or Stations (STA). All the STAs will share the same Internet connection via Vigor wireless router. The **General Settings** will set up the information of this wireless network, including its SSID as identification, located channel etc.



Security Overview

Real-time Hardware Encryption: Vigor Router is equipped with a hardware AES encryption engine so it can apply the highest protection to your data without influencing user experience.

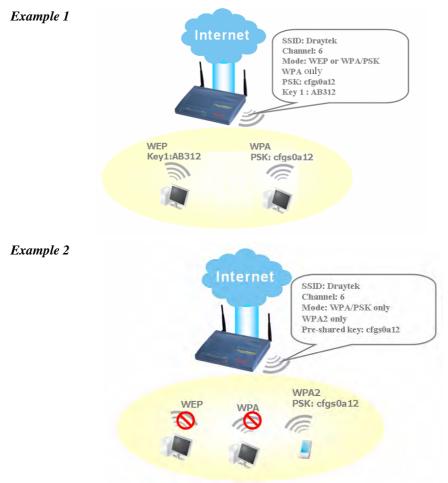
Complete Security Standard Selection: To ensure the security and privacy of your wireless communication, we provide several prevailing standards on market.

WEP (Wired Equivalent Privacy) is a legacy method to encrypt each frame transmitted via radio using either a 64-bit or 128-bit key. Usually access point will preset a set of four keys and it will communicate with each station using only one out of the four keys.

WPA(Wi-Fi Protected Access), the most dominating security mechanism in industry, is separated into two categories: WPA-personal or called WPA Pre-Share Key (WPA/PSK), and WPA-Enterprise or called WPA/802.1x.

In WPA-Personal, a pre-defined key is used for encryption during data transmission. WPA applies Temporal Key Integrity Protocol (TKIP) for data encryption while WPA2 applies AES. The WPA-Enterprise combines not only encryption but also authentication.

Since WEP has been proved vulnerable, you may consider using WPA for the most secure connection. You should select the appropriate security mechanism according to your needs. No matter which security suite you select, they all will enhance the over-the-air data protection and /or privacy on your wireless network. The Vigor wireless router is very flexible and can support multiple secure connections with both WEP and WPA at the same time.





Separate the Wireless and the Wired LAN- WLAN Isolation enables you to isolate your wireless LAN from wired LAN for either quarantine or limit access reasons. To isolate means neither of the parties can access each other. To elaborate an example for business use, you may set up a wireless LAN for visitors only so they can connect to Internet without hassle of the confidential information leakage. For a more flexible deployment, you may add filters of MAC addresses to isolate users' access from wired LAN.

Manage Wireless Stations - Station List will display all the station in your wireless network and the status of their connection.

Below shows the menu items for Wireless LAN.



3.12.2 General Settings

By clicking the **General Settings**, a new web page will appear so that you could configure the SSID and the wireless channel. Please refer to the following figure for more information.

Wireless LAN >> General Setup				
General Setting (IEEE 802.11)				
Enable Wireless LAN				
Mode :	Mixed(11b+11g)			
Index(1-15) in <u>Schedule</u> Setup:]		
SSID :	default			
Channel :	Channel 6, 2437MHz 🛛 🗸			
Note: If SuperG mode is en	abled, channel is fixed at 6.			
Hide SSIDLong Preamble				
Hide SSID : prevent SSID : Long Preamble : necessar	from being scanned. y for some older 802.11b devices or	nly (lowers performance).		
	OK Cancel			
Enable Wireless LAN	Check the box to	enable wireless function.		
Mode	Select an appropri	iate wireless mode.		
		+ SuperG) - The radio can support		
	-	EE802.11g and SuperG protocols		
	simultaneously.			
	_) - The radio can support both		
		IEEE802.11g protocols simultaneously. lio only supports SuperG.		
	-	dio only supports IEEE802.11g.		
	e •	dio only supports IEEE802.11b.		
	Mode :	Mixed(11b+11g)		
		Mixed(11b+11g+SuperG)		
		Mixed(11b+11g)		
		SuperG Only 11g Only		
		11b Only		
Index(1-15)	only. You may ch schedules pre-defi setup. The default	Set the wireless LAN to work at certain time interval only. You may choose up to 4 schedules out of the 15 schedules pre-defined in Applications >> Schedule setup. The default setting of this filed is blank and the function will always work.		
SSID	to a particular nan	The default SSID is "default". We suggest you change it to a particular name. It is the identification of the wireless LAN. SSID can be any text numbers or various special		
Channel		The channel of frequency of the wireless LAN. The default channel is 6. You may switch channel if the		

selected channel is under serious interference.

preamble with 56 bit sync filed instead of long preamble with 128 bit sync field. However, some original 11b wireless network devices only support long preamble.

Check it to use **Long Preamble** if needed to communicate with this kind of devices.

	selected challer is under serious interference.	
	Channel :	Channel 6, 2437MHz 🛛 👻
		Channel 1, 2412MHz
		Channel 2, 2417MHz
		Channel 3, 2422MHz
		Channel 4, 2427MHz
		Channel 5, 2432MHz
		Channel 6, 2437MHz
		Channel 7 , 2442MHz
		Channel 8, 2447MHz
		Channel 9, 2452MHz
		Channel 10, 2457MHz
		Channel 11, 2462MHz
		Channel 12, 2467MHz
		Channel 13, 2472MHz
Hide SSID	Check it to prevent from v	vireless sniffing and make it
	-	ients or STAs to join your
		3 2
		on the wireless utility, the user
	may only see the informat	ion except SSID or just cannot
	see any thing about Vigor	wireless router while site
	surveying.	
Long Preamble	This option is to define the	e length of the sync field in an
		e .
	ou2.11 packet. Most mode	ern wireless network uses short

Vigor2910 Series User's Guide

3.12.3 Security

Wireless LAN >> Security Settings

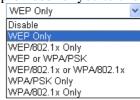
By clicking the **Security Settings**, a new web page will appear so that you could configure the settings of WEP and WPA.

/lode :	WEP Only
Set up RADIUS Se	rver if 802.1x is enabled.
NPA:	
Туре:	Mixed(WPA+WPA2) OWPA2 Only
Pre-Shared Key(PSK)	*****
Type 8~63 ASCII "cfgs01a2" or "0	character or 64 Hexadecimal digits leading by "Ox", for example x655abcd".
WEP:	
Encryption Mode:	64-Bit 💌
Use	WEP Key
○Key 1 :	*****
⊙Key 2 :	*****
○Кеу 3:	*****
○Key 4 :	******
For 64 bit WEP key Type 5 ASCII character '0x4142333132".	or 10 Hexadecimal digits leading by "0x", for example "AB312" or



OK Cancel

There are several modes provided for you to choose.



Disable - Turn off the encryption mechanism. **WEP Only -** Accepts only WEP clients and the encryption key should be entered in WEP Key. **WEP/802.1x Only -** Accept WEP clients with 802.1x authentication. Since the key will be auto-negotiated during authentication, the field of key setting below wi

during authentication, the field of key setting below will be not available for input. WEP or WPA/PSK - Accepts WEP and WPA clients

with legal key accordingly. Only Mixed (WPA+WPA2) is applicable if you select WPA/PSK.

WEP/802.1x or WPA/802.1x - Accept WEP or WPA clients with 802.1x authentication. Only

Mixed(WPA+WPA2) is applicable if you select WPA/PSK. Since the key will be auto-negotiated during authentication, the field of key setting below will be not available for input.

WPA/PSK Only - Accepts WPA clients and the encryption key should be entered in PSK. Remember to select WPA type to define either Mixed or WPA2 only in the field below.

WPA/802.1x Only - Accept WPA clients with 802.1x authentication. Remember to select WPA type to define

	either Mixed or WPA2 only in t key will be auto-negotiated duri field of key setting below will b	ng authentication, the
WPA	The WPA encrypts each frame to using the key, which either PSK field below or automatically neg- authentication. Type - Select from Mixed (WP Pre-Shared Key (PSK) - Either such as 012345678(or 64 Hexa 0x, such as "0x321253abcde")	C entered manually in this gotiated via 802.1x A+WPA2) or WPA2 only. r 8~63 ASCII characters, adecimal digits leading by
WEP	 64-Bit - For 64 bits WEP key, e such as 12345 (or 10 hexadecim such as 0x4142434445.) 128-Bit - For 128 bits WEP key characters, such as ABCDEFGF hexadecimal digits leading by 0 0x4142434445464748494A4B4 	nal digitals leading by 0x, y, either 13 ASCII HIJKLM (or 26 x, such as
	Encryption Mode:	64-Bit 64-Bit 128-Bit
	All wireless devices must suppo	ort the same WEP
	encryption bit size and have the	same key. Four keys can
	be entered here, but only one ke	-
	time. The keys can be entered in	n ASCII or Hexadecimal.
	Check the key you wish to use.	

3.12.4 Access Control

For additional security of wireless access, the **Access Control** facility allows you to restrict the network access right by controlling the wireless LAN MAC address of client. Only the valid MAC address that has been configured can access the wireless LAN interface. By clicking the **Access Control**, a new web page will appear, as depicted below, so that you could edit the clients' MAC addresses to control their access rights.

Vireless LAN >> Acce	iss Control	
Access Control		Set to Factory Default
🗹 Enable Access C	Control	
	Policy : Activate MAC address filter 💌	
	MAC Address Filter	
	Index Attribute MAC Address	
	Client's MAC Address :::::::	
	Attribute :	
	🔲 s: Isolate the station from LAN	
	Add Delete Edit Cancel	
	OK Clear All	

PolicySelect to enable any one of the following policy. Choose Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Isolate WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address list. Policy : Activate MAC address filter Isolate WLAN from LANMAC Address FilterDisplay all MAC addresses that are edited before. Four buttons (Add, Remove, Client's MAC Address - Manually enter the MAC address of wireless client.Attributes - select to isolate the wireless connection of the wireless client of the MAC address into the list.DeleteDelete the selected MAC address in the list.EditEdit the selected MAC address in the list.Give up the access control set up.	Enable Access Control	Select to enable the MAC Address access control feature.
Activate MAC address filter Isolate WLAN from LANMAC Address FilterDisplay all MAC addresses that are edited before. Four buttons (Add, Remove, Client's MAC Address - Manually enter the MAC address of wireless client.Attributes - select to isolate the wireless connection of the wireless client of the MAC address from LAN.AddAdd a new MAC address into the list.DeleteDelete the selected MAC address in the list.EditEdit the selected MAC address in the list.	Policy	Activate MAC address filter to type in the MAC addresses for other clients in the network manually. Choose Isolate WLAN from LAN will separate all the WLAN stations from LAN based on the MAC Address
Isolate WLAN from LANMAC Address FilterDisplay all MAC addresses that are edited before. Four buttons (Add, Remove, Client's MAC Address - Manually enter the MAC address of wireless client.Attributes - select to isolate the wireless connection of the wireless client of the MAC address from LAN.AddAdd a new MAC address into the list.DeleteDelete the selected MAC address in the list.EditEdit the selected MAC address in the list.		Policy : 🛛 Activate MAC address filter 😪
buttons (Add, Remove, Client's MAC Address - Manually enter the MAC address of wireless client.Attributes - select to isolate the wireless connection of the wireless client of the MAC address from LAN.AddAdd a new MAC address into the list.DeleteDelete the selected MAC address in the list.EditEdit the selected MAC address in the list.		
AddClient of the MAC address from LAN.AddAdd a new MAC address into the list.DeleteDelete the selected MAC address in the list.EditEdit the selected MAC address in the list.	MAC Address Filter	buttons (Add, Remove, Client's MAC Address - Manually enter the MAC
DeleteDelete the selected MAC address in the list.EditEdit the selected MAC address in the list.	Attribute	
Edit Edit the selected MAC address in the list.	Add	Add a new MAC address into the list.
	Delete	Delete the selected MAC address in the list.
Cancel Give up the access control set up.	Edit	Edit the selected MAC address in the list.
	Cancel	Give up the access control set up.

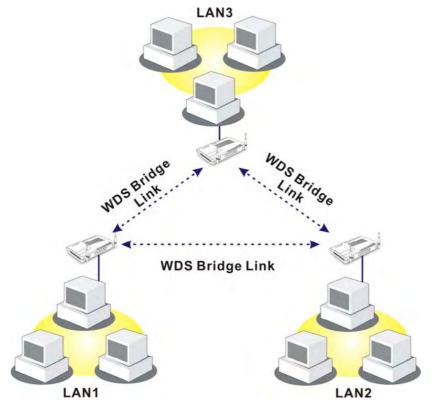
OK	Click it to save the access control list.
Clear All	Clean all entries in the MAC address list.

3.12.5 WDS

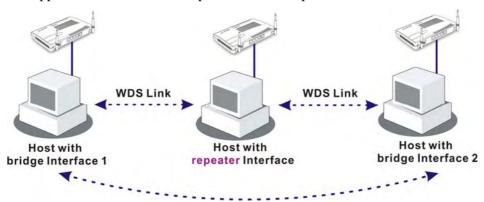
WDS means Wireless Distribution System. It is a protocol for connecting two access points (AP) wirelessly. Usually, it can be used for the following application:

- Provide bridge traffic between two LANs through the air.
- Extend the coverage range of a WLAN.

To meet the above requirement, two WDS modes are implemented in Vigor router. One is **Bridge**, the other is **Repeater**. Below shows the function of WDS-bridge interface:

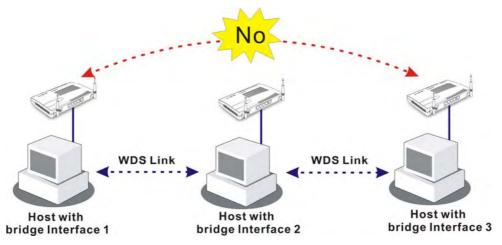


The application for the WDS-Repeater mode is depicted as below:



The major difference between these two modes is that: while in **Repeater** mode, the packets received from one peer AP can be repeated to another peer AP through WDS links. Yet in **Bridge** mode, packets received from a WDS link will only be forwarded to local wired or wireless hosts. In other words, only Repeater mode can do WDS-to-WDS packet forwarding.

In the following examples, hosts connected to Bridge 1 or 3 can communicate with hosts connected to Bridge 2 through WDS links. However, hosts connected to Bridge 1 CANNOT communicate with hosts connected to Bridge 3 through Bridge 2.



Click WDS from Wireless LAN menu. The following page will be shown.

NDS Settings	Set to Factory Defau
	Bridge
Mode: Disable 💙	Enable Peer MAC_Address
Security:	
• Disable	
WEP:	
Use the same WEP key set in <u>Security</u>	
Settings.	
Encryption Mode 🚦 64-bit 👻	Note: Disable unused links to get better
Key index : 1	performance.
The key index is fixed if the security mode is not	Repeater
"WEP Only".	Enable Peer MAC Addess
Kev : *********	
The key format is the same as the one used in	
Security Settings.	
	Access Point Function:
	Enable
Pre-shared Key:	
Type : TKIP	Status:
Key :	Send "Hello" message to peers.
Type 8~63 ASCII characters or 64 hexadecimal	Link Status
digits leading by "0x", for example "cfgs01a2" or "0x655abcd".	Note: The status is valid only when the peer also supports this function.

Wireless LAN >> WDS Settings

Mode

Choose the mode for WDS setting. **Disable** mode will not invoke any WDS setting. **Bridge** mode is designed to fulfill the first type of application. **Repeater** mode is for the second one.

Mode:

Disable	*
Disable	
Bridge	
Repeate	r

Security	There are three types for security, Disable , WEP and Pre-shared key . The setting you choose here will make the following WEP or Pre-shared key field valid or not. Choose one of the types for the router.
WEP	Check this box to use the same key set in Security Settings page. If you did not set any key in Security Settings page, this check box will be dimmed.
Settings	 Encryption Mode - If you checked the box of Use the same WEP key, you do not need to choose 64-bit or 128-bit as the Encryption Mode. If you do not check that box, you can set the WEP key now in this page. Key Index - Choose the key that you want to use after selecting the proper encryption mode. Key - Type the content for the key.
Pre-shared Key	Type 8 ~ 63 ASCII characters or 64 hexadecimal digits leading by " $0x$ ".
Bridge	If you choose Bridge as the connecting mode, please type in the peer MAC address in these fields. Six peer MAC addresses are allowed to be entered in this page at one time. Yet please disable the unused link to get better performance. If you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Repeater	If you choose Repeater as the connecting mode, please type in the peer MAC address in these fields. Two peer MAC addresses are allowed to be entered in this page at one time. Similarly, if you want to invoke the peer MAC address, remember to check Enable box in the front of the MAC address after typing.
Access Point Function	Click Enable to make this router serving as an access point; click Disable to cancel this function.
Status	It allows user to send "hello" message to peers. Yet, it is valid only when the peer also supports this function.

3.12.6 AP Discovery

Vigor router can scan all regulatory channels and find working APs in the neighborhood. Based on the scanning result, users will know which channel is clean for usage. Also, it can be used to facilitate finding an AP for a WDS link. Notice that during the scanning process (about 5 seconds), no client is allowed to connect to Vigor.

This page is used to scan the existence of the APs on the wireless LAN. Yet, only the AP which is in the same channel of this router can be found. Please click **Scan** to discover all the connected APs.

Access Point List				
	BSSID	Channel	SSID	
		Scan		
See <u>St</u>	atistics.			
	uring the scanning e router.	process (~5 seco	nds), no station is allowed to	o connect
Add to	WDS Settings :			
AP's MA	AC address	: : : : :	: : Add	

If you want the found AP applying the WDS settings, please type in the AP's MAC address on the bottom of the page and click **Add**. Later, the MAC address of the AP will be added to the page of WDS setting.

3.12.7 Station List

Station List provides the knowledge of connecting wireless clients now along with its status code. There is a code summary below for explanation. For convenient **Access Control**, you can select a WLAN station and click **Add to Access Control** below.

Wireless LAN >> Station List

	Status MAC Address
	Refresh
	Status Codes :
	C: Connected, No encryption. E: Connected, WEP.
	P: Connected, WPA.
	A: Connected, WPA2.
	B: Blocked by Access Control. N: Connecting.
	F: Fail to pass 802.1X or WPA/PSK authentication.
	Note: After a station connects to the router successfully, it may be turned off without notice. In that case, it will still be on the list until the
	connection expires.
	Add to <u>Access Control</u> :
	Client's MAC address
	Add
Refresh	Click this button to refresh the status of stat
44	Click this button to add ourset calcoted M
Add	Click this button to add current selected MA

3.12.8 Station Rate Control

This page allows you to control the upload and download rate of each wireless client (station). Please check the box of **Enable** to invoke this setting. The range for the rate is between $100 \sim 30,000$ kbps.

Wireless LAN >> Station Rate Control							
Station R	Station Rate Control						
Enabl	е						
	Upload Rate :	300	00 Kbps				
	Download Rate :	300	00 Kbps				
	Note: 1. Range: 100~30,000 Kbps, Increment: 2. The specified rates are applied to eac		vireless client.				
	ОК	Cancel					

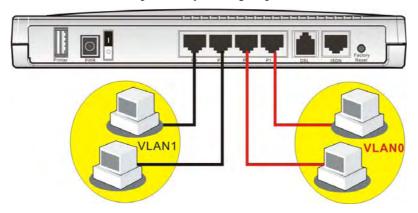
3.13 VLAN

Virtual LAN function provides you a very convenient way to manage hosts by grouping them based on the physical port.

VLAN	
Wired VLAN	
Wireless VLAN	
VLAN Cross Setup	
Wireless Rate Control	

3.13.1 Wired VLAN

PCs connected to Ethernet ports of the router can be divided into different groups and formed VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.



The VLAN >> Wired VALN allows you to configure VLAN settings through wired connection to achieve the above intention. Simply check P1 and P2 boxes on the line of VLAN0; and check P3 and P4 boxes on the line of VLAN1.

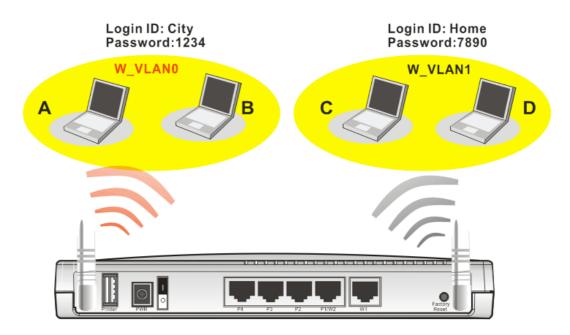
VLAN >> Wired VLAN Configuration

🗹 Enable								
	P1	P2	P3	P4				
VLAN0	✓							
VLAN1								
VLAN2								
VLAN3								
Enable	OK		Cancel					
Lnadie		ck this box to enal figuration).	ble this function (IOT VLAN				
D1 D4	Cha	P1 – P4 Check the box to make the computer connecting to the port being grouped in specified VLAN. Be aware that each port can be grouped in different VLAN at the same time only if you check the box. For example, if you check the boxes of VLAN0-P1 and VLAN1-P1, you can make P1 to be grouped under VLAN0 and VLAN1 simultaneously.						
P1 – P4	bein can l you VLA	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLA	ified VLÂN. Be a erent VLAN at th r example, if you N1-P1, you can n	aware that each port ne same time only if check the boxes of nake P1 to be grouped				
P1 – P4 VLAN0-3	being can l you VLA unde	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLA	ified VLAN. Be a erent VLAN at th r example, if you N1-P1, you can n AN1 simultaneo	aware that each port ne same time only if check the boxes of nake P1 to be grouped usly.				
	being can b you VLA unde This interface has b	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLAI or VLAN0 and VL router allows you	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo to set 4 groups of P1 boxes will a	aware that each port he same time only if check the boxes of hake P1 to be grouped usly. of virtual LAN. serve as WAN				
VLAN0-3 Note: If WAN2	being can b you VLA unde This interface has b nnot be checke	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLAI or VLAN0 and VL router allows you	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo to set 4 groups of P1 boxes will a	aware that each port he same time only if check the boxes of hake P1 to be grouped usly. of virtual LAN. serve as WAN				
VLAN0-3 Note: If WAN2 interface and car	being can b you VLA unde This interface has b nnot be checke	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLAI or VLAN0 and VL router allows you	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo to set 4 groups of P1 boxes will a	aware that each port he same time only if check the boxes of hake P1 to be grouped usly. of virtual LAN. serve as WAN				
VLAN0-3 Note: If WAN2 interface and car Wired VLAN Configurat	being can b you VLA unde This interface has b nnot be checke	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLAI or VLAN0 and VL router allows you	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo to set 4 groups of P1 boxes will a	aware that each port he same time only if check the boxes of hake P1 to be grouped usly. of virtual LAN. serve as WAN				
VLAN0-3 Note: If WAN2 interface and car Wired VLAN Configurat	being can b you VLA unde This interface has b nnot be checke	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLAI or VLAN0 and VL router allows you been enabled, the d as shown in th	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo a to set 4 groups of P1 boxes will a e following dia	aware that each port ne same time only if check the boxes of nake P1 to be grouped usly. of virtual LAN. serve as WAN gram.				
VLAN0-3 Note: If WAN2 interface and car Wired VLAN Configurat	being can b you VLA unde This interface has b nnot be checke	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLAI or VLAN0 and VL router allows you been enabled, the d as shown in th	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo to set 4 groups of P1 boxes will a e following dia	aware that each port he same time only if check the boxes of hake P1 to be grouped usly. of virtual LAN. serve as WAN gram.				
VLAN0-3 Note: If WAN2 interface and car Wired VLAN Configurat VLAN0	being can b you VLA unde This interface has b nnot be checke	g grouped in spec be grouped in diff check the box. Fo NO-P1 and VLA1 or VLAN0 and VL router allows you been enabled, the d as shown in th	ified VLAN. Be a erent VLAN at the r example, if you N1-P1, you can n AN1 simultaneo to set 4 groups of P1 boxes will a e following dia P3	aware that each port a same time only if check the boxes of nake P1 to be grouped usly. of virtual LAN. serve as WAN gram.				

3.13.2 Wireless VLAN

PCs (equipped with wireless network cards) connected to the router through wireless interface can be divided into different groups and formed W_VLAN. PCs under the same groups can share each other information through the router and will not be peeked by other groups.

PCs under the same groups can use same Login ID and password to access into Internet. For example, see the following graphic. Both A and B use the same login ID (City) and password (1234). Therefore, they are grouped in the same W_VLAN.



The VLAN >> Wireless VALN allows you to configure Wireless VLAN settings through wireless connection to achieve the above intention. Simply type Login ID and password with City and 1234 in the boxes of W_VLAN0. And type Login ID and password with Home and 7890 in the boxes of W_VLAN1. Users can configure fifteen groups of wireless VLAN in this page.

VLAN >> Wireless VLAN Setup

🗹 Enable						View <u>Online </u>	Station Table
W_VLAN	Login ID	Password	Attributes	W_VLAN	Login ID	Password	Attributes
0	City	1234	Details	8			Details
1	Home	7890	Details	9			Details
2			Details	10			Details
3			Details	11			Details
4			Details	12			Details
5			Details	13			Details
6			Details	14			Details
7			Details	15			Details
🔄 Disabl	e broadcast a	nd multicast tra	affic.				
lotes: . Login ID . Disable hroughput . Login VF	: 1~11 chara broadcast and t will be reduc RL for wireless	cters, Password I multicast traff ed.	l: 1~11 char ic to maximi:	ze wireless \		; however, the	WLAN
lotes: . Login ID . Disable hroughput . Login VF	: 1~11 chara broadcast and t will be reduc RL for wireless	cters, Password I multicast traff ed. clients: ogin.htm or ht	l: 1~11 char ic to maximi: tp://(Vigor IP OK	ze wireless \ Address)/ lo Cancel	gin.htm	; however, the	

1

Activated Date: Expired Date: Connect all WDS links with this VLAN group. Tsolate each member in this VLAN group. Cancel Activated Date – Use the drop down lists to set the active date for the wireless VLAN. The wireless VLAN function be available when the time is arrival. Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
Expired Date: Connect all WDS links with this VLAN group. Tsolate each member in this VLAN group. Cancel Activated Date – Use the drop down lists to set the active date for the wireless VLAN. The wireless VLAN function be available when the time is arrival. Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
✓ Isolate each member in this VLAN group. OK Cancel Activated Date – Use the drop down lists to set the activ date for the wireless VLAN. The wireless VLAN function be available when the time is arrival. Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
Activated Date – Use the drop down lists to set the active date for the wireless VLAN. The wireless VLAN function be available when the time is arrival. Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
Activated Date – Use the drop down lists to set the activ date for the wireless VLAN. The wireless VLAN function be available when the time is arrival. Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
date for the wireless VLAN. The wireless VLAN function be available when the time is arrival. Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival.						
date for the wireless VALN. This function will be invalid when the time is arrival.						
date for the wireless VALN. This function will be invalid when the time is arrival.	Expired Date – Use the drop down lists to set the expired date for the wireless VALN. This function will be invalid when the time is arrival					
when the time is arrival.						
	thic					
	. uns					
box to activate this connection.	1					
Isolate each member in this VLAN group – Check this						
to isolate all the members in this VLAN group and not all	low					
the information sharing among them.						
Disable broadcast and multicast trafficCheck this box to prevent broadcast and multicast traffic forwarding to all W_VLAN.						

How can you (wireless client) access into Internet?

After finishing the configuration of wireless VLAN, the wireless clients connecting to this router must do the following steps to access into Internet.

- 1. Open a browser and type http://www.draytek.vlan/login.htm or http://(vigor router's IP address)/login.htm on the address line.
- 2. The following screen will appear.

Fek Wireless VLAN
City
••••

3. Type in Login ID and Password that was configured in Wireless VLAN Setup page. In this case, we choose the configuration set in first group of W_VLAN (City and 1234).

4. When the accessing is successful, the following screen will appear.

		~
🗿 http://192.168.1.1 - DrayTek Wireless 🔳 🗖 🔀		
Connection time: 00:00:13 Logout		
Connection time: 000019		
	DrayTek Wireless VLAN	
Link Status:Active		
	User login succeeds !!!	
🕘 完成 🔮 網際網路 🛒		
	Copyright © 2005, DrayTek Corp. All Rights Reserved.	
		×

Note: The floating window with connection time will be shown on the screen till you logout.

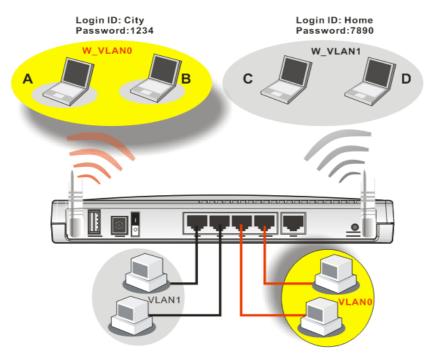
5. You can go to **Diagnostics>>Wireless VLAN Online Station** for viewing the connection status whenever you want.

Diagnostics >> Wireless VLAN Online Station

Wireless VLAN Onl	ine Station Table		<u>Refresh</u>
IP Address	MAC Address	Login ID	<u>▲</u>
192.168.1.15 192.168.1.16	00-14-85-26-00-8C 00-0E-35-18-14-E7	City Home	
			~

3.13.3 VLAN Cross Setup

This function allows the router to integrate VLAN and W_VLAN for managing different computers (notebooks). See the following picture for an example. With VLAN Cross Setup, notebook A/B and PCs on VLAN0 can share resources without difficulty.



The VLAN >> VALN Cross Setup allows you to set a communication bridge between computers in Wireless VLAN and wired VLAN. To achieve the intention of the above illustration, simply check the box under VLAN0 on the line of W_VLAN0.

inable				
	VLAN0	VLAN1	VLAN2	VLAN3
W_VLANO	~			
W_VLAN1				
W_VLAN2				
W_VLAN3				
W_VLAN4				
W_VLAN5				
W_VLAN6				
W_VLAN7				
W_VLAN8				
W_VLAN9				
W_VLAN10				
W_VLAN11				
W_VLAN12				
W_VLAN13				
W_VLAN14				
W_VLAN15				
WDS				
II WDS links belon	VLAN i, see Wireles g to the same VLAN i, see Wired VLAN S		ils.	

VLAN >> VLAN Cross Setup

ΟK Cancel

Enable	Check this box to invoke VLAN Cross Setup function.
VLAN0-3	It represents the groups of virtual LAN connected by Ethernet interface.
W_VLAN0-15	It represents the groups of wireless VLAN communicated by wireless interface.

3.13.4 Wireless Rate Control

Rate Control manages the transmission rate of data in and out through the router. You can also manage the in/out rate of each wireless VLAN. Go to VLAN menu and select Wireless Rate Control. The following page will appear. Click Enable to invoke VLAN function.

For the rate control of wireless connection, please open VLAN menu and choose Wireless Rate Control. The following page will be shown for you to adjust.

VLAN >>	Wireless	VLAN	Rate	Control

✓Enable				Range :	100∼30,000 Kbp	s, Increment : 100 Kbp
W_VLAN	Upload Rate (Kbp	s) Download F	Rate (Kbps)	W_VLAN	Upload Rate (Kbps)	Download Rate (Kbps)
0	300 00	300	00	8	300 00	300 00
1	300 00	300	00	9	300 00	300 00
2	300 00	300	00	10	300 00	300 00
З	300 00	300	00	11	300 00	300 00
4	300 00	300	00	12	300 00	300 00
5	300 00	300	00	13	300 00	300 00
6	300 00	300	00	14	300 00	300 00
7	300 00	300	00	15	300 00	300 00
lote: Spe	cified rate is an a	aggregate rate	e for the VL	AN group.		

Enable	Check this box to enable this function (for Rate Control). The rate control will limit the transmission rate for upload and download.
Upload Rate	It decides the rate of data transmission for output. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.
Download Rate	It decides the rate of data transmission for input. The default setting is 300. The range must be between 100 kbps to 20,000kbps. Adjust the values according to your necessity.

3.14 System Maintenance

For the system setup, there are several items that you have to know the way of configuration: Status, Administrator Password, Configuration Backup, Syslog, Time setup, Reboot System, Firmware Upgrade.

Below shows the menu items for System Maintenance.

System Maintenance
System Status
▶ TR-069
Administrator Password
Configuration Backup
SysLog / Mail Alert
Time and Date
Management
Reboot System
🕨 Firmware Upgrade

3.14.1 System Status

The **System Status** provides basic network settings of Vigor router. It includes LAN and WAN interface information. Also, you could get the current running firmware version or firmware related information from this presentation.

System Status

Aodel Name Firmware Version Build Date/Time	: DrayTek Vigor : 3.0.7_RC4 : Thu Jul 26 15::			
	System			WAN 1
CPU Usage	:3%		Link Status	: Connected
Total Memory	: 16M		MAC Address	: 00-50-7F-DD-15-19
Memory usage	: 29 %		Connection	: Static IP
		,	IP Address	: 172.16.3.229
	LAN		Default Gateway	: 172.16.3.4
MAC Address	: 00-50-7F-	DD-15-18		
1st IP Address				
1st Subnet Mask				
DHCP Server	: Yes			
DNS	: 194.109.6	.66		
	VoIP			
Port	: 1	2		
SIP registrar	:			
Account ID	:	change_me		
	change_me	change_me		
Register	:			
Codec	:			
In Calls	: 0	0		
Out Calls	: 0	0		

Firmware Version Build Date/Time MAC Address 1st IP Address

1st Subnet Mask

Display the firmware version of the router.Display the date and time of the current firmware build.Display the MAC address of the LAN Interface.Display the IP address of the LAN interface.Display the subnet mask address of the LAN interface.

DHCP Server	Display the current status of DHCP server of the LAN interface.
MAC Address	Display the MAC address of the WAN Interface.
IP Address	Display the IP address of the WAN interface.
Default Gateway	Display the assigned IP address of the default gateway.
DNS	Display the assigned IP address of the primary DNS.
MAC Address	Display the MAC address of the wireless LAN.
Frequency Domain	It can be Europe (13 usable channels), USA (11 usable channels) etc. The available channels supported by the wireless products in different countries are various.
Firmware Version	It indicates information about equipped WLAN miniPCi card. This also helps to provide availability of some features that are bound with some WLAN miniPCi card.

3.14.2 TR-069 Setting

Vigor router with TR-069 is available for matching with VigorACS server. Such page provides VigorACS and CPE settings under TR-069 protocol. All the settings configured here is for CPE to be controlled and managed with VigorACS server. Users need to type URL, username and password for the VigorACS server that such device will be connected. However URL, username and password under CPE client are fixed that users cannot change it. The default CPE username and password are "vigor" and "password". You will need it when you configure VigorACS server.

ACS Server	
URL	
Username	
Password	
CPE Client	
URL	http://172.16.3.229/cwm/CRN.html
Port	80
Username	vigor
Password	•••••
Inform Settings	
O Disable	
 Enable 	
Interval Time	900 second(s)
	OK

System Maintenance >> TR-069 Setting

URL

Type the URL for VigorACS server. If the connected CPE needs to be authenticated, please set URL as the following and type username and password for VigorACS server: http://{IP address of

	<pre>VigorACS}:8080/ACSServer/services/ACSServlet If the connected CPE does not need to be authenticated please set URL as the following: http://{IP address of VigorACS}:8080/ACSServer/services/UnAuthACSServ let</pre>
Username/Password	Type username and password for ACS Server for authentication. For example, if you want to use such CPE with VigorACS, you can type as the following: Username: acs Password: password
Periodic Inform Settings	 Disable – The system will not send inform message to ACS server. Enable – The system will send inform message to ACS server periodically (with the time set in the box of interval time).

3.14.3 Administrator Password

This page allows you to set new password.

System Maintenance >> Administrator Password Setup

Administrator Password				
Old Password				
New Password				
Confirm Password				

OK

Old Password	Type in the old password. The factory default setting for password is blank.
New Password	Type in new password in this filed.
Confirm New Password	Type in the new password again.

When you click OK, the login window will appear. Please use the new password to access into the web configurator again.

3.14.4 Configuration Backup

Backup the Configuration

Follow the steps below to backup your configuration.

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup

Configuration	Backup / Restoration
Restoration	
	Select a configuration file.
	Browse.
	Click Restore to upload the file.
	Restore
Backup	
	Click Backup to download current running configurations as a file.
	Backup Cancel

2. Click **Backup** button to get into the following dialog. Click **Save** button to open another dialog for saving configuration as a file.

File Do	wnload 🔀
?	You are downloading the file: config.cfg from 192,168.1.1 Would you like to open the file or save it to your computer? Open Save Cancel More Info Always ask before opening this type of file

3. In **Save As** dialog, the default filename is **config.cfg**. You could give it another name by yourself.

Save As						? 🗙
Save in:	🞯 Desktop		~	00	1	
My Recent Documents Desktop My Documents	My Documeni My Computer My Network F RVS-COM Lite Annex A MWSnap300 TeleDanmark Tools Config V2k2_232_cc V2k6_250_cc	Places				
	File name:	config			~	Save
My Network	Save as type:	Configuration file			~	Cancel

4. Click **Save** button, the configuration will download automatically to your computer as a file named **config.cfg**.

The above example is using **Windows** platform for demonstrating examples. The **Mac** or **Linux** platform will appear different windows, but the backup function is still available.

Note: Backup for Certification must be done independently. The Configuration Backup does not include information of Certificate.

Restore Configuration

1. Go to **System Maintenance** >> **Configuration Backup**. The following windows will be popped-up, as shown below.

System Maintenance >> Configuration Backup			
Configuration	Configuration Backup / Restoration		
Restoration			
	Select a configuration file. Browse., Click Restore to upload the file. Restore		
Backup	Click Backup to download current running configurations as a file.		

- 2. Click **Browse** button to choose the correct configuration file for uploading to the router.
- 3. Click **Restore** button and wait for few seconds, the following picture will tell you that the restoration procedure is successful.

3.14.5 Syslog/Mail Alert

SysLog function is provided for users to monitor router. There is no bother to directly get into the Web Configurator of the router or borrow debug equipments.

System Maintenance >> SysLog / Mail Alert Setup			
SysLog / Mail Alert Setup			
SysLog Access Setup		Mail Alert Setup	
🗹 Enable		📃 Enable	
Router Name		SMTP Server	
Server IP Address		Mail To	
Destination Port 514		Return-Path	
Enable syslog message:		Authentication	
🗹 Firewall Log		User Name	
🗹 VPN Log		Password	
User Access Log			
Call Log WAN Log			
WAN LOY Router/DSL information			
OK Clear Cancel			
Cnable	Click "Enable" to activate this function.		
Router Name	Assign a name for the router.		
erver IP	The IP address of the Syslog server.		
Destination Port	Assign a port for the Syslog protocol.		

Enable syslog message	Check the box listed on this web page to send the corresponding message of firewall, VPN, User Access, Call, WAN, Router/DSL information to Syslog.
SMTP Server	The IP address of the SMTP server.
Mail To	Assign a mail address for sending mails out.
Return-Path	Assign a path for receiving the mail from outside.
Authentication	Check this box to activate this function while using e-mail application.
User Name	Type the user name for authentication.
Password	Type the password for authentication.
~	

Click **OK** to save these settings.

For viewing the Syslog, please do the following:

- 1. Just set your monitor PC's IP address in the field of Server IP Address
- 2. Install the Router Tools in the **Utility** within provided CD. After installation, click on the **Router Tools>>Syslog** from program menu.

💼 Router Tools V2.5 4	👔 🔊 About Router Tools
	📲 Ez Configurator Vigor2100 Series
	📫 🌺 Firmware Upgrade Utility
	111/ Syslog
	🛛 📝 Uninstall Router Tools V2.5.4
	🕘 Visit DrayTek Web Site

3. From the Syslog screen, select the router you want to monitor. Be reminded that in **Network Information**, select the network adapter used to connect to the router. Otherwise, you won't succeed in retrieving information from the router.

ontrols		192.168.1 Vigor serie		WAN Status Gateway IP (Fixed		
LAN Status TX Pao 96		RX Pack 759	ets	WAN IP (Fixed)	RX Packet	s TX Rate
rewall Log VPN On Line Routers -	Log User Acces	s Log Ca	ll Log WAN Lo Host Name:	<u></u>	n Net State	
IP Address 192.168.1.1	Mask 255.255.255.0	MAC 00-50-	NIC Descriptio	Reduck R 15015	9 Family PCI Fast E Default Geteway:	themet NIC - : 💌
			IP Address:	192.168.1.10	DHCP Server:	192.168.1.1
			Subnet Mask:	255.255.255.0	Lease Obtained:	Wed Apr 06 16:59:40 2005
<	R	> efresh	DNS Servers:	168.95.1.1 192.168.1.1	Lease Expires:	Sat Apr 09 16:59:40 2005
DSL Status	Charl		Up Grand	Davis Canad	CND Mauria	
Mode	Stat	8	Up Speed	Down Speed	SNR Margin	Loop Att

3.14.6 Time and Date

It allows you to specify where the time of the router should be inquired from.

Time Information				
Current System Time 2006	Jun 12 Mon 8 : 45 : 0			
Time Setup				
🔘 Use Browser Time				
💿 Use Internet Time Client				
Time Protocol	NTP (RFC-1305) 🔽			
Server IP Address	pool.ntp.org			
Time Zone	(GMT) Greenwich Mean Time : Dublin			
Enable Daylight Saving				
Automatically Update Interval	30 min 🔽			
Current System Time	Click Inquire Time to get the current time.			
se Browser Time	Select this option to use the browser time from the remote administrator PC host as router's system time.			
	Select to inquire time information from Time Server on the Internet using assigned protocol.			
se Internet Time	1			
	1			
ïme Protocol	the Internet using assigned protocol.			
'ime Protocol erver IP Address	the Internet using assigned protocol. Select a time protocol.			
'ime Protocol erver IP Address 'ime Zone	the Internet using assigned protocol. Select a time protocol. Type the IP address of the time server.			
Jse Internet Time Time Protocol erver IP Address Time Zone Cnable Daylight Saving Automatically Update Interva	the Internet using assigned protocol.Select a time protocol.Type the IP address of the time server.Select the time zone where the router is located.Such function is useful for some area.			

3.14.7 Management

This page allows you to manage the settings for access control, access list, port setup, and SNMP setup. For example, as to management access control, the port number is used to send/receive SIP message for building a session. The default value is 5060 and this must match with the peer Registrar when making VoIP calls.

Management Access Contr	ol	Management Port Setu	IP
Management Access Contr Allow management fro FTP Server HTTP Server HTTPS Server Telnet Server SSH Server Disable PING from the Access List List IP 1 2 3	om the Internet Internet Subnet Mask	 User Define Ports Telnet Port HTTP Port HTTPS Port FTP Port SSH Port SNMP Setup Enable SNMP Age Get Community Set Community Manager Host IP 	 Default Ports 23 (Default: 23) 80 (Default: 80) 443 (Default: 443 21 (Default: 21) 22 (Default: 22)
		Trap Community Notification Host IP	public
			10
		Trap Timeout	10 seconds

System Maintenance >> Management	System	Maintenance	>>	Management
----------------------------------	--------	-------------	----	------------

Allow management from the Internet	Enable the checkbox to allow system administrators to login from the Internet. There are several servers provided by the system to allow you managing the router from Internet. Check the box(es) to specify.
Disable PING from the Internet	Check the checkbox to reject all PING packets from the Internet. For security issue, this function is enabled by default.
Access List	You could specify that the system administrator can only login from a specific host or network defined in the list. A maximum of three IPs/subnet masks is allowed. List IP - Indicate an IP address allowed to login to the router. Subnet Mask - Represent a subnet mask allowed to login to the router.
User Defined Ports	Check to specify user-defined port numbers for the Telnet and HTTP servers.
Default Ports	Check to use standard port numbers for the Telnet and HTTP servers.
Enable SNMP Agent	Check it to enable this function.
Get Community	Set the name for getting community by typing a proper character. The default setting is public.

Set Community	Set community by typing a proper name. The default setting is private.
Manager Host IP	Set one host as the manager to execute SNMP function. Please type in IP address to specify certain host.
Trap Community	Set trap community by typing a proper name. The default setting is public.
Notification Host IP	Set the IP address of the host that will receive the trap community.
Trap Timeout	The default setting is 10 seconds.

3.14.8 Reboot System

The Web Configurator may be used to restart your router. Click **Reboot System** from **System Maintenance** to open the following page.

System Maintenance >> Reboot System Reboot System				
	Osing current configuration			
	O Using factory default configuration			
<u> </u>	OK			

If you want to reboot the router using the current configuration, check **Using current** configuration and click **OK**. To reset the router settings to default values, check **Using** factory default configuration and click **OK**. The router will take 5 seconds to reboot the system.

3.14.9 Firmware Upgrade

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools. The following web page will guide you to upgrade firmware by using an example. Note that this example is running over Windows OS (Operating System).

Download the newest firmware from DrayTek's web site or FTP site. The DrayTek web site is www.draytek.com (or local DrayTek's web site) and FTP site is ftp.draytek.com.

Click System Maintenance>> Firmware Upgrade to launch the Firmware Upgrade Utility.

Web Firmware (Jpgrade			
Select a f	īrmware file.			
			Browse	
Click Upgr	ade to upload the file.	Upgrade		
TFTP Firmware	Upgrade from LAN			
Current F	rmware Version: 3.1.0			

Firmware Upgrade Procedures:

- 1. Click "OK" to start the TFTP server.
 2. Open the Firmware Upgrade Utility or other 3-party TFTP client software.
- 3. Check that the firmware filename is correct.
- 4. Click "Upgrade" on the Firmware Upgrade Utility to start the upgrade.
- 5. After the upgrade is compelete, the TFTP server will automatically stop running.

Do you want to upgrade firmware ? OK

Click **OK**. The following screen will appear. Please execute the firmware upgrade utility first.

System Maintenance >> Firmware Upgrade



For the detailed information about firmware update, please go to Chapter 4.

3.15 Diagnostics

Diagnostic Tools provide a useful way to **view** or **diagnose** the status of your Vigor router. Below shows the menu items for Diagnostics.



3.15.1 Dial-out Trigger

Click **Diagnostics** and click **Dial-out Trigger** to open the web page. The internet connection (e.g., ISDN, PPPoE, PPPoA, etc) is triggered by a package sending from the source IP address.

Diagnostics >> Dial-out Trigger

HEX Format:	
00 00 00 00 00 00-00 00 00 00 00 00 00	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00-00 00 00 00 00 00 0	
00 00 00 00 00 00 00 00-00 00 00 00 00 0	
Decoded Format:	
0.0.0.0 -> 0.0.0.0	
Pr 0 len 0 (0)	

Decoded FormatIt shows the source IP address (local), destination IP
(remote) address, the protocol and length of the package.RefreshClick it to reload the page.

3.15.2 Routing Table

Click **Diagnostics** and click **Routing Table** to open the web page.

```
Diagnostics >> View Routing Table
```

```
Current Running Routing Table | Refresh |

Key: C - connected, S - static, R - RIP, * - default, ~ - private

* 0.0.0.0/ 0.0.0.0 via 172.16.3.1, WAN1

C~ 192.168.1.0/ 255.255.255.0 is directly connected, LAN

C 172.16.3.0/ 255.255.255.0 is directly connected, WAN1
```

Refresh

Click it to reload the page.

3.15.3 ARP Cache Table

Click **Diagnostics** and click **ARP Cache Table** to view the content of the ARP (Address Resolution Protocol) cache held in the router. The table shows a mapping between an Ethernet hardware address (MAC Address) and an IP address.

Diagnostics >> View ARP Cache Table

thernet ARP Cache	Table	<u>Clear</u> <u>Refresh</u>
IP Address	MAC Address	
192.168.1.10	00-0E-A6-2A-D5-A1	
172.16.3.112	00-40-CA-6B-56-BA	
172.16.3.132	00-05-5D-E4-ED-86	
172.16.3.20	00-0D-60-6F-83-BC	
172.16.3.121	00-0C-6E-E7-79-99	
172.16.3.141	00-11-2F-C7-39-0B	
172.16.3.133	00-50-7F-23-4D-B1	
172.16.3.179	00-11-2F-4B-15-F2	
172.16.3.21	00-05-5D-A1-2B-FF	
172.16.3.2	00-11-D8-68-0D-AE	
172.16.3.18	00-50-FC-2F-3D-17	
172.16.3.151	00-50-7F-2F-33-FF	
172.16.3.19	00-0D-60-6F-89-CA	

Refresh

Clear

Click it to reload the page.

Click it to clear the whole table.

3.15.4 DHCP Table

The facility provides information on IP address assignments. This information is helpful in diagnosing network problems, such as IP address conflicts, etc.

Click **Diagnostics** and click **DHCP Table** to open the web page.

DHCP IP A	ssignment Table			Re	fresh
Index	ver: Running IP Address 192.168.1.10	MAC Address 00-0E-&6-2&-D5-&1	Leased Time 0:00:02.630	HOST ID ok-lccgjyiy075u	
ndex		It dis	plays the conn	ection item numb	▼ er.
P Addr	ess		plays the IP ad	dress assigned by	this router fo
IAC A	ddress		plays the MAC P assigned IP	C address for the s address for it.	pecified PC tl
eased '	Time	It dis	It displays the leased time of the specified PC.		

HOST ID It displays the host ID name of the specified PC.

Refresh Click it to reload the page.

3.15.5 NAT Sessions Table

Click Diagnostics and click NAT Sessions Table to open the setup page.

Diagnostics >> NAT Sessions Table

s Table					Refr
:Port	#Pseudo Port	Peer IP	:Port	Interface	
2491	 52078	24.9.93.189	443		
2493	52080	207.46.25.2	80	WAN1	
3079	52665	207.46.5.10	80	WAN1	
	:Port	:Port #Pseudo Port 2491 52078 2493 52080	:Port #Pseudo Port Peer IP 2491 52078 24.9.93.189 2493 52080 207.46.25.2	:Port #Pseudo Port Peer IP :Port 2491 52078 24.9.93.189 443 2493 52080 207.46.25.2 80	:Port #Pseudo Port Peer IP :Port Interface 2491 52078 24.9.93.189 443 WAN1 2493 52080 207.46.25.2 80 WAN1

Private IP:Port It indicates the source IP address and port of local PC.

#Pseudo Port It indicates the temporary port of the router used for NAT.

Peer IP:Port	It indicates the destination IP address and port of remote host.
Interface	It indicates the interface of the WAN connection.
Refresh	Click it to reload the page.

3.15.6 Wireless VLAN Online Station Table

Diagnostics >> Wireless VLAN Online Station

Click **Diagnostics** and click **Wireless VLAN Online Station Table to** open the web page. It will display the IP address, MAC address and Login ID information for all the Wireless VLAN stations.

eless VLAN Onli	ne Station Table		Refres
P Address	MAC Address	Login ID	
92.168.1.15	00-14-85-26-00-8C	City	
92.168.1.16	00-0E-35-A8-A4-E7	Home	

IP Address	Display the IP address of the wireless station.
MAC Address	Display the MAC address of the wireless station.
Login ID	Display the login ID that the wireless station belongs to.

3.15.7 Data Flow Monitor

This page displays the running procedure for the IP address monitored and refreshes the data in an interval of several seconds. The IP address listed here is configured in Bandwidth Management. You have to enable IP bandwidth limit and IP session limit before invoke Data Flow Monitor. If not, a notification dialog box will appear to remind you enabling it.

Limit Session			
0	🔊 Enabl	e 🔘 Disable	
De	efault M	ax Sessions: 100	
Li	mitation	List	
I	ndex	Start IP	End IP

Click **Diagnostics** and click **Data Flow Monitor** to open the web page. You can click **IP Address**, **TX rate**, **RX rate** or **Session** link for arranging the data display.

Diagnostics >> Data Flow Monitor

🔲 Enable Data Flow Monitor

		Refresh Se	econds: 10 💌 Page: 1	*	<u>Refresh</u>
Index	IP Address	<u>TX rate(Kbps)</u>	<u>RX_rate(Kbps)</u> 🛩	Sessions	Action

Note: 1. Click "Block" to prevent specified PC from surfing Internet for 5 minutes.

2. The IP blocked by the router will be shown in red, and the session column will display the remaining time that the specified IP will be blocked.

Enable Data Flow Monitor Refresh Seconds Check this box to enable this function.

Use the drop down list to choose the time interval of refreshing data flow that will be done by the system automatically.

Refresh Seconds: 5 🔽

5
10
15
30

Refresh	Click this link to refresh this page manually.			
Index	Display the number of the data flow.			
IP Address	Display the IP address of the monitored device.			
TX rate (kbps)	Display the transmission speed of the monitored device.			
RX rate (kbps)	Display the receiving speed of the monitored device.			
Sessions	Display the session number that you specified in Limit Session web page.			
Action	Block - can prevent specified PC accessing into Internet withi minutes.			
	5) Sessions Action			
	1 / 100 <u>Block</u>			

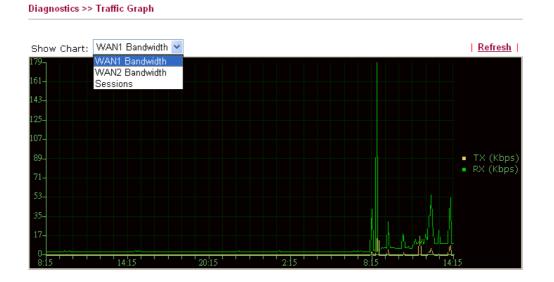
Unblock – the device with the IP address will be blocked in five

minutes. The remaining time will be shown on the session column.



3.13.8 Traffic Graph

Click **Diagnostics** and click **Traffic Graph** to pen the web page. Choose WAN1 Bandwidth/WAN2 Bandwidth or Sessions for viewing different traffic graph. Click **Refresh** to renew the graph at any time.



The horizontal axis represents time. Yet the vertical axis has different meanings. For WAN1/WAN2 Bandwidth chart, the numbers displayed on vertical axis represent the numbers of the transmitted and received packets in the past.

For Sessions chart, the numbers displayed on vertical axis represent the numbers of the NAT sessions during the past.

3.15.9 Ping Diagnosis

Click **Diagnostics** and click **Ping Diagnosis** to pen the web page.

```
Diagnostics >> Ping Diagnosis
```

which WA	N ping through, p	LAN PC or you don't want to spe ease select "Unspecified".	ecify
Ping tr Ping tr Result	irough: WAN1 Host / IP GateWay1 GateWay2 DNS	IP Address:	<u>Clear</u>
			X

Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the router automatically. Ping through: Unspecified Unspecified WAN1 WAN2
Ping to	Use the drop down list to choose the destination that you would like to ping.
IP Address	Type in the IP address of the Host/IP that you want to ping.
Run	Click this button to start the ping work. The result will be displayed on the screen.
Clear	Click this link to remove the result on the window.

3.15.10 Trace Route

Click **Diagnostics** and click **Trace Route** to open the web page. This page allows you to trace the routes from router to the host. Simply type the IP address of the host in the box and click **Run**. The result of route trace will be shown on the screen.

Diagnostics >> Trace Route

Trace through:	WAN1 🔽	
Host / IP Address:		Run
Result		<u>Clear</u>
traceroute to 172.16 1 Request timed ou 2 Request timed ou Trace complete.	it. *	

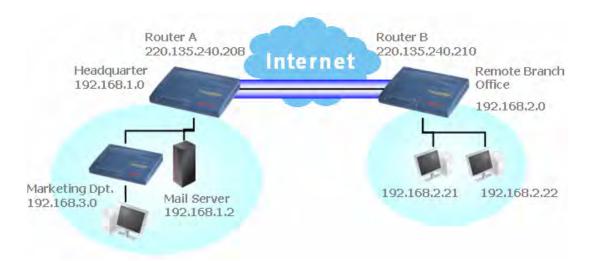
Ping through	Use the drop down list to choose the WAN interface that you want to ping through or choose Unspecified to be determined by the router automatically.	
Host/IP Address	It indicates the IP address of the host.	
Run	Click this button to start route tracing work.	
Clear	Click this link to remove the result on the window.	

This page is left blank.

4 Application and Examples

4.1 Create a LAN-to-LAN Connection Between Remote Office and Headquarter

The most common case is that you may want to connect to network securely, such as the remote branch office and headquarter. According to the network structure as shown in the below illustration, you may follow the steps to create a LAN-to-LAN profile. These two networks (LANs) should NOT have the same network address.



Settings in Router A in headquarter:

VPN and Remote Access >> PPP General Setun

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then,

For using **PPP** based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup		
PPP/MP Protocol	IP Address Assignment fo	or Dial-In Users
Dial-In PPP Authentication PAP or CHAP V	Start IP Address	192.168.1.200
Dial-In PPP Encryption Optional MPPE		
Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to

set general settings in **IPSec General Setup**, such as the pre-shared key that both parties have known.

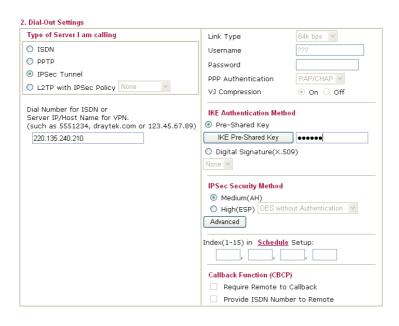
VPN and Remote Access >> IPSec General Setup		
VPN IKE/IPSec General Setup		
Dial-in Set up for Remote Dial-in users and Dynamic IP Client (LAN to LAN).		
IKE Authentication Method		
Pre-Shared Key		
Confirm Pre-Shared Key		
IPSec Security Method		
Medium (AH)		
Data will be authentic, but will not be encrypted.		
High (ESP) ▼ DES ▼ 3DES ▼ AES Data will be encrypted and authentic.		
OK Cancel		

- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

Profile Index : 1 1. Common Settings	
Profile Name Branch1	Call Direction 🛛 💿 Both 🔿 Dial-Out 🔿 Dial-In
Enable this profile	🔲 Always on
	Idle Timeout 300 second(s)
VPN Connection Through: WAN1 First 🌱	Enable PING to keep alive
	PING to the IP

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.



If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 🗸
O ISDN	Username	draytek
PPTP	Password	•••••
O IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	💿 On 🔘 Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Metho Pre-Shared Key	d
220.135.240.210	IKE Pre-Shared Key	•••••
	 Digital Signature(X.50 	19)
	None 🗸	
	IPSec Security Method	
	Medium(AH)	
	O High(ESP) DES with	out Authentication 🔽
	Advanced	
	Index(1-15) in <u>Schedule</u>	
	Callback Function (CBCP	·
	Provide ISDN Numb	

6. Set **Dial-In settings** to as shown below to allow Router B dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

3. Dial-In Settings	
Allowed Dial-In Type	
ISDN	Username ???
РРТР	Password
☑ IPSec Tunnel	VJ Compression 💿 On 🔿 Off
L2TP with IPSec Policy None	
	IKE Authentication Method
Specify ISDN CLID or Remote VPN Gateway	Pre-Shared Key
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key
220.135.240.210	Digital Signature(X.509)
or Peer ID	None 😽
	IPSec Security Method
	Medium (AH)
	High (ESP)
	🗹 DES 🗹 3DES 🗹 AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget 0 minute(s)

If a *PPP-based service* is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

3. Dial-In Settings	
Allowed Dial-In Type	
ISDN ISDN	Username draytek
PPTP	Password ••••••
🔲 IPSec Tunnel	VJ Compression 💿 On 🔿 Off
L2TP with IPSec Policy None	IKE Authentication Method
	Pre-Shared Key
Specify ISDN CLID or Remote VPN Gateway Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key
220.135.240.210	Digital Signature(X.509)
or Peer ID	None 💌
	IPSec Security Method
	Medium (AH)
	High (ESP)
	DES V 3DES V AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget minute(s)

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router A can direct the packets destined to the remote network to Router B via the VPN connection.

4. TCP/IP Network Settings	1	
My WAN IP	0.0.0.0	RIP Direction Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP	192.168.2.0	Route 🛩
Remote Network Mask	255.255.255.0	
	More	Change default route to this VPN tunnel (Only single WAN supports this)
	ОК	Clear Cancel

Settings in Router B in the remote office:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using **PPP based** services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup		
PPP/MP Protocol	IP Address Assignment f	or Dial-In Users
Dial-In PPP Authentication PAP or CHAP 💌	Start IP Address	192.168.2 200
Dial-In PPP Encryption Optional MPPE		
Mutual Authentication (PAP) 🛛 🔘 Yes 💿 No		
Username		
Password		

For using **IPSec-based** service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IPSec General Setup**, such as the pre-shared key that both

parties have known.

N IKE/IPSec General Setup		
al-in Set up for Remote Dial-in users	s and Dynamic IP Client (LAN to LAN).	
IKE Authentication Method		
Pre-Shared Key	••••	
Confirm Pre-Shared Key	•••••	
IPSec Security Method		
🗹 Medium (AH)		
Data will be authentic, but	t will not be encrypted.	
High (ESP) 🛛 🔽 DES 📝	3DES 🗹 AES	
Data will be encrypted and	d authentic.	

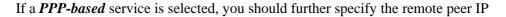
- 3. Go to LAN-to-LAN. Click on one index number to edit a profile.
- 4. Set **Common Settings** as shown below. You should enable both of VPN connections because any one of the parties may start the VPN connection.

1. Common Settings		
Profile Name	Branch1	Call Direction 💿 Both 🔿 Dial-Out 🔿 Dial-In
Enable this profile		🔲 Always on
VPN Connection Through: WAN1 First 💌		Idle Timeout 300 second(s)
		Enable PING to keep alive
		PING to the IP

5. Set **Dial-Out Settings** as shown below to dial to connect to Router B aggressively with the selected Dial-Out method.

If an *IPSec-based* service is selected, you should further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-Out connection.

2. Dial-Out Settings	
Type of Server I am calling	Link Type 64k bps 🔽
O ISDN	Username ???
О РРТР	Password
IPSec Tunnel	PPP Authentication PAP/CHAP
C L2TP with IPSec Policy None	VJ Compression On Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Method Pre-Shared Key
220.135.240.208	IKE Pre-Shared Key
	 Digital Signature(X.509)
	None 🗸
	IPSec Security Method Medium(AH) High(ESP) DES without Authentication Advanced Index(1-15) in <u>Schedule</u> Setup: Callback Function (CBCP)
	Require Remote to Callback
	Provide ISDN Number to Remote



Address, Username, Password, PPP Authentication and VJ Compression for this Dial-Out connection.

Z. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 👻
O ISDN	Username	draytek
PPTP	Password	
O IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	⊙ On ◯ Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Metho	
220.135.240.208	IKE Pre-Shared Key	
	Digital Signature(X.50	9)
	None 🛩	
	IDC Cltr. Mathad	
	IPSec Security Method	
	Medium(AH) Medium(AH)	ut Authentication
	O High(ESP) DES witho	at Authentication
	Advanced	
	Index(1-15) in Schedule	Setun:
		,
	Callback Function (CBCP)	
	🗌 Require Remote to (Callback
	Provide ISDN Number	er to Remote

6. Set **Dial-In settings** to as shown below to allow Router A dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

3. Dial-In Settings	
Allowed Dial-In Type	
ISDN	Username ???
РРТР	Password
☑ IPSec Tunnel	VJ Compression 💿 On 🔿 Off
L2TP with IPSec Policy None	IKE Authentication Method
Specify ISDN CLID or Remote VPN Gateway	✓ Pre-Shared Key
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key
220.135.240.208	Digital Signature(X.509)
or Peer ID	None 💙
	IPSec Security Method
	Medium (AH)
	High (ESP)
	🗹 DES 🗹 3DES 🗹 AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Budget 0 minute(s)

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

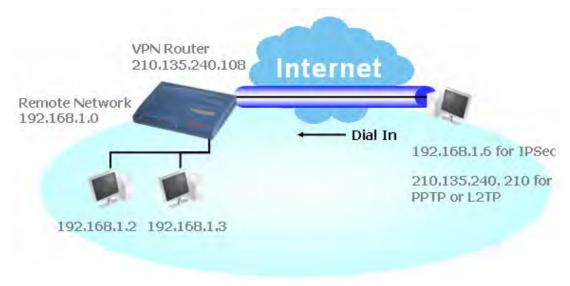
. Dial-In Settings Allowed Dial-In Type		
	Username draytek	
	Password	
IPSec Tunnel	VJ Compression 💿 On 🔘 Off	
L2TP with IPSec Policy None	IKE Authentication Method	
Specify ISDN CLID or Remote VPN Gateway	🗹 Pre-Shared Key	
Peer ISDN Number or Peer VPN Server IP	IKE Pre-Shared Key	
220.135.240.208	Digital Signature(X.509)	
or Peer ID	None 👻	
	IPSec Security Method	
	🗹 Medium (AH)	
	High (ESP)	
	🗹 DES 🗹 3DES 🗹 AES	
	Callback Function (CBCP)	
	Enable Callback Function	
	Use the Following Number to Callback	:
	Callback Number	
	Callback Budget 0 minute	e(s)

7. At last, set the remote network IP/subnet in **TCP/IP Network Settings** so that Router B can direct the packets destined to the remote network to Router A via the VPN connection.

4. TCP/IP Network Settings	;		
My WAN IP	0.0.0.0	RIP Direction	Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to ren do	note network, you have to
Remote Network IP	192.168.1.0		Route 💌
Remote Network Mask	255.255.255.0		
	More	Change default route single WAN supports this	to this VPN tunnel (Only)
	ОК С	lear Cancel	

4.2 Create a Remote Dial-in User Connection Between the Teleworker and Headquarter

The other common case is that you, as a teleworker, may want to connect to the enterprise network securely. According to the network structure as shown in the below illustration, you may follow the steps to create a Remote User Profile and install Smart VPN Client on the remote host.



Settings in VPN Router in the enterprise office:

- 1. Go to **VPN and Remote Access** and select **Remote Access Control** to enable the necessary VPN service and click **OK**.
- 2. Then, for using PPP based services, such as PPTP, L2TP, you have to set general settings in **PPP General Setup**.

PPP General Setup		
PPP/MP Protocol	IP Address Assignment for Dial-	n Users
Dial-In PPP Authentication	Start IP Address	192.168.1.200
Dial-In PPP Encryption Optional MPPE		
Mutual Authentication (PAP) 🛛 🔿 Yes 💿 No		
Username		
Password		

For using IPSec-based service, such as IPSec or L2TP with IPSec Policy, you have to set general settings in **IKE/IPSec General Setup**, such as the pre-shared key that both parties have known.

VPN and Remote Access >> IPSec Gene	ral Setup	
VPN IKE/IPSec General Setup Dial-in Set up for Remote Dial-in users	and Dynamic IP Client (LAN	to LAN)
IKE Authentication Method		
Pre-Shared Key	••••	
Confirm Pre-Shared Key	••••	
IPSec Security Method		
Medium (AH)		
Data will be authentic, but	will not be encrypted.	
High (ESP) ☑ DES ☑ Data will be encrypted and	3DES 🗹 AES authentic.	
	OK Cancel	

- 3. Go to **Remote Dial-In Users**. Click on one index number to edit a profile.
- 4. Set **Dial-In** settings to as shown below to allow the remote user dial-in to build VPN connection.

If an *IPSec-based* service is selected, you may further specify the remote peer IP Address, IKE Authentication Method and IPSec Security Method for this Dial-In connection. Otherwise, it will apply the settings defined in **IPSec General Setup** above.

2. Dial-Out Settings		
Type of Server I am calling	Link Type	64k bps 👻
O ISDN	Username	???
О РРТР	Password	
IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	On Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Metho	d
210.135.240.210	IKE Pre-Shared Key	
	Digital Signature(X.50	9)
	None 🛩	
	IPSec Security Method	
	 Medium(AH) High(ESP) DES without 	ut Authentication
	Advanced	dr /
	Auvanceu	
	Index(1-15) in <u>Schedule</u>	Setup:
	Callback Function (CBCP	
	Require Remote to	
	Provide ISDN Numbe	er to Remote

If a *PPP-based* service is selected, you should further specify the remote peer IP Address, Username, Password, and VJ Compression for this Dial-In connection.

Type of Server I am calling	Link Type	64k bps 🖌
O ISDN	Username	draytek
• РРТР	Password	
🔘 IPSec Tunnel	PPP Authentication	
O L2TP with IPSec Policy None	VJ Compression	⊙ On ◯ Off
Dial Number for ISDN or Server IP/Host Name for VPN. (such as 5551234, draytek.com or 123.45.67.89)	IKE Authentication Metl Pre-Shared Key	rod
210.135.240.210	IKE Pre-Shared Key	
	O Digital Signature(X.5	.09)
	IPSec Security Method	
	 Medium(AH) High(ESP) DES wit 	hout Authentication
	Advanced	Autorite autori
	Index(1-15) in <u>Schedul</u>	,
	Callback Function (CBC	
	Require Remote to	
	Provide ISDN Num	ber to Remote

Settings in the remote host:

- 1. For Win98/ME, you may use "Dial-up Networking" to create the PPTP tunnel to Vigor router. For Win2000/XP, please use "Network and Dial-up connections" or "Smart VPN Client", complimentary software to help you create PPTP, L2TP, and L2TP over IPSec tunnel. You can find it in CD-ROM in the package or go to www.draytek.com download center. Install as instructed.
- 2. After successful installation, for the first time user, you should click on the **Step 0**. **Configure** button. Reboot the host.

order to configure a L2	ProhibitIpSec registry valu 2TP/IPSec connection usin	
	For more infomation, plea oft Knowledgement Base	
	Configure	
	Contigure	
Step 1. Dial to ISP		
	otten a public IP, you car	n skip this step.
	otten a public IP, you car	n skip this step. Dial
If you have already g		
If you have already g		

3. In Step 2. Connect to VPN Server, click Insert button to add a new entry.

If an IPSec-based service is selected as shown below,

Session Name:	Office	
VPN Server IP/HO	ST Name(s	uch as 123.45.67.89 or draytek.com)
192.168.1.1		
User Name :	die re	
Password :		×
Type of VPN		
OPPTP		OLZTP
IPSec Tuni	nel	OL2TP over IPSec
PPTP Encryption No encryp Require an	hom	
(Maximum)		
Use default	gateway (on remote network

You may further specify the method you use to get IP, the security method, and authentication method. If the Pre-Shared Key is selected, it should be consistent with the one set in VPN router.

My IP :	172.16.3.10	0			v
Type of IPSe	с.			-	-
O Standard	d IPSec Tunnel				
Remot	e Subnet :	<u>U</u>			
Remot	e Subnet Mask (255	~55	::55	Ū.
💿 Virture I	P Dray	Tek Virtun	e Interi	face	*
💿 Obt	ain an IP address a	automatic	ally (DH	HCP ov	er IPSec
OSpe	cify an IP address	_			-
IP .	Address:	LS.	160		200
Sul	bnet Mask:		100 P	100	Ū.
Security Meth	hod				
Security Meth		High(ES	P)		
		High(ES	P)		*
O Medium(AH) (P)		*
O Medium(AH) (<u>P)</u>		*
Medium(MBS Authority Me	AH) (P)		*
MBS Authority Me • Pre-shar	AH)		P)	Bro	×

If a PPP-based service is selected, you should further specify the remote VPN server IP address, Username, Password, and encryption method. The User Name and Password should be consistent with the one set up in the VPN router. To use default gateway on remote network means that all the packets of remote host will be directed to VPN server then forwarded to Internet. This will make the remote host seem to be working in the enterprise network.

Session Name:	office	
VPN Server IP/HC)ST Name(s	uch as 123.45.67.89 or draytek.com)
192.168.1.1		
User Name :	draytek	_user1
Password :	****	
Type of VPN		
• PPTP		OL2TP
O IPSec Tun	nel	OL2TP over IPSec
PPTP Encryption O No encryp O Require en O Maximum	ition ncryption	cryption
		n remote network

4. Click **Connect** button to build connection. When the connection is successful, you will find a green light on the right down corner.

4.3 QoS Setting Example

Assume a teleworker sometimes works at home and takes care of children. When working time, he would use Vigor router at home to connect to the server in the headquater office downtown via either HTTPS or VPN to check email and access internal database. Meanwhile, children may chat on VoIP or Skype in the restroom.

1. Make sure the QoS Control on the left corner is checked. And select BOTH in **Direction**.

Enable the QoS Control)TH 🔽
WAN Inbou OU	T idth
	TH widt

 Enter the Name of Index Class 1 by clicking Edit link. In this index, the user will set reserve bandwidth for Email using protocol POP3 and SMTP.
 Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
Class Ru Inde		N	ame				Rule	Service	
	ж	N	ame				Rule <u>Edit</u>	Service	
Inde	9 X 5 1	N	ame					Service <u>Edit</u>	Туре

 Enter the Name of Index Class 2 by clicking Edit link. In this index, the user will set reserve bandwidth for HTTPS. And click Basic button on the right. Bandwidth Management >> Quality of Service

Index	Status	Bandwidth	Directon	Class 1	Class 2	Class 3	Others	UDP Bandwidth Control	
WAN1	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	Setup
WAN2	Enable	10000Kbps/10000Kbps	Outbound	25%	25%	25%	25%	Inactive	<u>Setup</u>
Class Ri Inde		N	ame				Rule	Service	Туре
	вх	N	ame				Rule <u>Edit</u>	Service	Гуре
	ex 5 1	N	ame					Service <u>Edit</u>	

4. Click **Setup** link for WAN1. Check **Enable UDP Bandwidth Control** on the bottom to prevent enormous UDP traffic of VoIP influent other application.

Bandwidth Management >> Quality of Service

₩AN1 General Set ▼Enable the QoS	•	
W	AN Inbound Bandwidth	10000 Kbps
w	AN Outbound Bandwidth	10000 Kbps
Index	Class Name	Reserved_bandwidth Ratio
Class 1	E-mail	25 %
Class 2	НТТР	25 %
Class 3		25 %
	Others	25 %
Enable UDP Ba	ndwidth Control	Limited_bandwidth Ratio 25 %
		Online Statistic

5. If the worker has connected to the headquater using host to host VPN tunnel. (Please refer to Chapter 3 VPN for detail instruction), he may set up an index for it. Enter the Class Name of Index 3. In this index, he will set reserve bandwidth for 1 VPN tunnel.

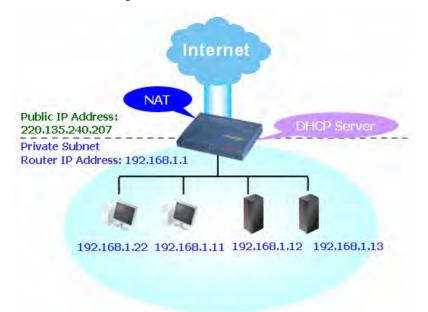


6. Click edit to open a new window. First, check the ACT box. Then click **SrcEdit** to set a worker's subnet address. Click **DestEdit** to set headquarter's subnet address. Leave other fields and click OK.

4.4 LAN - Created by Using NAT

LAN >> General Setup

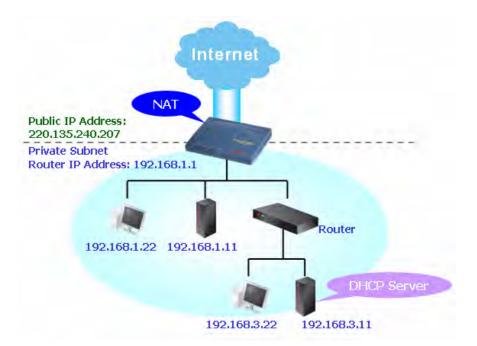
An example of default setting and the corresponding deployment are shown below. The default Vigor router private IP address/Subnet Mask is 192.168.1.1/255.255.255.0. The built-in DHCP server is enabled so it assigns every local NATed host an IP address of 192.168.1.x starting from 192.168.1.10.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

AN IP Network Configurat	ion	DHCP Server Configuration			
For NAT Usage		💿 Enable Server 🔘 Disal	ble Server		
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Sul	bnet 🔾 2nd Subnet		
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10		
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50		
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1		
2nd Subnet Mask	255.255.255.0 d Subnet DHCP Server	DHCP Server IP Address for Relay Agent DNS Server IP Address			
RIP Protocol Control	Disable 👻	Force DNS manual s	etting		
		Secondary IP Address			

To use another DHCP server in the network rather than the built-in one of Vigor Router, you have to change the settings as show below.



You can just set the settings wrapped inside the red rectangles to fit the request of NAT usage.

LAN >> General Setup

Ethernet TCP / IP and DHCI	^o Setup		
LAN IP Network Configurat	ion	DHCP Server Configuration	1
For NAT Usage		🔘 Enable Server 💿 Disab	ole Server
1st IP Address	192.168.1.1	Relay Agent: 🔘 1st Sub	onet 🔾 2nd Subnet
1st Subnet Mask	255.255.255.0	Start IP Address	192.168.1.10
For IP Routing Usage 🔘	Enable 💿 Disable	IP Pool Counts	50
2nd IP Address	192.168.2.1	Gateway IP Address	192.168.1.1
2nd Subnet Mask	255.255.255.0	DHCP Server IP Address	
2n	d Subnet DHCP Server	for Relay Agent DNS Server IP Address	
		🔲 Force DNS manual s	etting
RIP Protocol Control	Disable 🚩	Primary IP Address	
		Secondary IP Address	

4.5 Calling Scenario for VoIP function

4.5.1 Calling via SIP Sever

Example 1: Both John and David have SIP Addresses from different service providers.

John's SIP URL: 1234@draytel.org, David's SIP URL: 4321@iptel.org

Settings for John

DialPlan index 1 Phone Number: 1111 Display Name: David SIP URL: 4321@iptel.org

🗹 Enable				
Phone Nu	mber	1111		
Display N	ame	David		
SIP URL		4321		@ iptel.org
Loop thro	ugh	None 🔽		
Backup P	ione Number			
VoIP >> SIP Accounts	OK	Clear	r(Cancel
SIP Account Index No. 1				
Profile Name	drayte1	<u> </u>	(11	char max.)
Register via	Auto	¥	make ca	II without register
SIP Port	5060			
Domain/Realm	dravtel o	ra		(63 char may)

draytel.org

1 hour 🕑 3600

VoIP1 VoIP2 ISDN

OK Cancel

None 🔽

1 🗸

proxy

Johr

1234

SIP Accounts Settings ---

Profile Name: draytel1 Register via: Auto SIP Port: 5060 (default) Domain/Realm: draytel.org Proxy: draytel.org Act as outbound proxy: unhecked Display Name: John Account Number/Name: 1234 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF --- John ca

(Use default value)

Settings for David

DialPlan index 1 Phone Number:2222 Display Name: John SIP URL:1234@draytel.org

SIP Accounts Settings ----

Profile Name: iptel 1 Register via: Auto SIP Port: 5060(default) Domain/Realm: iptel.org Proxy: iptel.org Act as outbound proxy: unchecked Display Name: David Account Name: 4321 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF ----

(Use default value)

John calls David ---

Act as outbound

Account Number/Name

Authentication ID

NAT Traversal Support

Display Name

Password

Expiry Time

Ring Port

Ring Patterr

He picks up the phone and dials 1111#. (DialPlan Phone Number for David)

(63 char max.)

(63 char max.)

(63 char max.)

(63 char max.)

(23 char max.)

sec

🗹 Enable		
	Phone Number	2222
	Display Name	John
	SIP URL	1234 @ draytel.org
	Loop through	None 🛩
	Backup Phone Number	

Profile Name	iptel 1 (11 cha	ar max.)
Register via	Auto 💌 🗌 make call v	vithout register
SIP Port	5060	
Domain/Realm	iptel.org	(63 char max.)
Proxy	iptel.org	(63 char max.)
🗌 Act as outbound p	iroxy	
Display Name	David (23 cha	ar max.)
Account Number/Name	4321	(63 char max.)
Authentication ID		(63 char max.)
Password	••••	(63 char max.)
Expiry Time	1 hour 🔽 3600 sec	
NAT Traversal Support	None 🖌	
Ring Port	VoIP1 VoIP2 ISDN	
Ring Pattern	1 🛩	

David calls John

VoIP >> SIP Account

He picks up the phone and dials 2222# (DialPlan Phone Number for John)

OK Cancel

Example 2: Both John and David have SIP Addresses from the same service provider.

John's SIP URL: 1234@draytel.org , David's SIP URL: 4321@draytel.org

Settings for John

DialPlan index 1 Phone Number: 1111 Display Name: David SIP URL: 4321@draytel.org

SIP Accounts Settings ----

Profile Name: draytel 1 Register via: Auto SIP Port: 5060 (default) Domain/Realm: draytel.org Proxy: draytel.org Act as outbound proxy: unchecked Display Name: John Account Number/Name: 1234 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF ----

(Use default value)

Settings for David

DialPlan index 1 Phone Number:2222 Display Name: John SIP URL:1234@draytel.org

SIP Accounts Settings ----

Profile Name: John Register via: Auto SIP Port: 5060(default) Domain/Realm: draytel.org Proxy: iptel.org Act as outbound proxy: unchecked Display Name: David Account Name: 4321 Authentication ID: unchecked Password: **** Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Enable	Phone Number	1111		
	Display Name	David		
	SIP URL	4321	@ draytel.org	
	Loop through	None 👻		
	Backup Phone Number			
oIP >> SIP Ac	OK	Clear	Cancel	

Profile Name	draytel 1		(11 char m	hax.)
Register via	Auto 💌	mai	ke call with	out register
SIP Port	5080			
Domain/Realm	draytel.org			(63 char max.)
Proxy	draytel.org			(63 char max.)
Act as outbound p	локу			
Display Name	John		(23 char m	iax.)
Account Number/Name	1234			(63 char max.)
Authentication ID				(63 char max.)
Password	****			(63 char max.)
Expiry Time	1 hour 💌	3600	sec	
NAT Traversal Support	None 😽			
Ring Part	VoIP1	VoIP2	ISON	
Ring Pattern	1 ~			

John calls David

He picks up the phone and dials 1111#. (DialPlan Phone Number for David) Or, He picks up the phone and dials 4321#. (David's Account Name)

✓ Enable		
Phone Number	2222	
Display Name	John	
SIP URL	1234	@ draytel.org
Loop through	None 💌	
Backup Phone No	umber	
olP >> SIP Accounts		
Profile Name	draytel 1	11 char max.)
Register via		call without register
SIP Port	5060	
Domain/Realm	draytel.org	(63 char max.)
Proxy	draytel.org	(63 char max.)
Act as outbound p	ouced	
		23 char max.)
Act as outbound p		23 char max.) (63 char max.)
Act as outbound p Display Name	David (2	
Act as outbound p Display Name Account Number/Name	David (2 4321	(63 char max.)
Act as outbound y Display Name Account Number/Name Authentication ID Password Expiry Time	David (2	(63 char max.) (63 char max.)
Act as outbound j Display Name Account Number/Name Authentication ID Password Expiry Time NAT Traversal Support	David (2 4321 1 hour 💌 3600 None 💌	(63 char max.) (63 char max.) (63 char max.) sec
Act as outbound y Display Name Account Number/Name Authentication ID Password Expiry Time	David (2 4321 1 heur 💌 [3600	(63 char max.) (63 char max.) (63 char max.) sec

David calls John

He picks up the phone and dials 2222# (DialPlan Phone Number for John) Or, He picks up the phone and dials 1234# (John's Account Name)

4.5.2 Peer-to-Peer Calling

Example 3: Arnor and Paulin have Vigor routers respectively, they can call each other *without* SIP Registrar. First they must have each other's IP address and assign an Account Name for the port used for calling.

Arnor's SIP URL: 1234@214.61.172.53

Settings for Arnor

DialPlan index 1 Phone Number: 1111 Display Name: paulin SIP URL: 4321@ 203.69.175.24

SIP Accounts Settings ---

Profile Name: Paulin Register via: None SIP Port: 5060(default) Domain/Realm: (blank) Proxy: (blank) Act as outbound proxy: unchecked Display Name: Arnor Account Name: 1234 Authentication ID: unchecked Password: (blank) Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Settings for Paulin

DialPlan index 1 Phone Number:2222 Display Name: Arnor SIP URL: 1234@214.61.172.53

SIP Accounts Settings ----

Profile Name: Arnor Register via: None SIP Port: 5060(default) Domain/Realm: (blank) Proxy: (blank) Act as outbound proxy: unchecked Display Name: Paulin Account Name: 4321 Authentication ID: unchecked Password: (blank) Expiry Time: (use default value)

CODEC/RTP/DTMF---

(Use default value)

Paulin's SIP URL: 4321@ 203.69.175.24

Enable	
Phone Number	1111
Display Name	paulin
SIP URL	4321 @ 203.69.175.24
Loop through	None V
Backup Phone Nur	mber
	OK Clear Cancel
oIP >> SIP Accounts	
IP Account Index No. 1	
Profile Name	Paulin (11 char max.)
Register via	None 🔽 🔲 make call without register
SIP Port	5060
SIP Port Domain/Realm	5060 (63 char max.)
Domain/Realm	(63 char max.) (63 char max.)
Domain/Realm Proxy	(63 char max.) (63 char max.)
Domain/Realm Proxy Act as outbound p	(63 char max.) (63 char max.)
Domain/Realm Proxy Act as outbound p Display Name	(63 char max.) (63 char max.) roxy [Amor (23 char max.)
Domain/Realm Proxy Act as outbound p Display Name Account Number/Name	(63 char max.) (63 char max.) proxy Amor (23 char max.) 1234 (63 char max.)
Domain/Realm Proxy Display Name Account Number/Name Authentication ID	(63 char max.) (63 char max.) oroxy Amor (23 char max.) 1234 (63 char max.) (63 char max.)
Domain/Realm Proxy Display Name Account Number/Name Authentication ID Password	(63 char max.) (63 char max.) (63 char max.) (63 char max.) (63 char max.) (63 char max.) (63 char max.)
Domain/Realm Proxy Display Name Account Number/Name Authentication ID Password Expiry Time	(63 char max.) (63 char max.) Amor (23 char max.) 1234 (63 char max.) (63 char max.) (63 char max.) (63 char max.) 1 hour 3000 sec

OK Cancel

Arnor calls Paulin

He picks up the phone and dials **1111#**. (DialPlan Phone Number for Arnor)

VolP >> DialP	lan Setup	
Phone Book	Index No. 1	
🗹 Enable		
	Phone Number	2222
	Display Name	Amor
	SIP URL	1234 @214.61.172.53
	Loop through	None 💌
	Backun Phone Number	

VoIP >> SIP Accounts

Profile Name	Arnor	(11 char max.)
Register via	None 🔽 🔲 mał	e call without register
SIP Port	5060	
Domain/Realm		(63 char max.)
roxy		(63 char max.)
🗌 Act as outbound p	roxy	
Display Name	Paulin	(23 char max.)
ccount Number/Name	4321	(63 char max.)
Authentication ID		(63 char max.)
Password		(63 char max.)
Expiry Time	1 hour 💌 3600	sec
NAT Traversal Support	None 🔽	
Ring Port	VoIP1 VoIP2	ISDN
Ring Pattern	1 🕶	

Paulin calls Arnor

He picks up the phone and dials **2222**# (DialPlan Phone Number for John)

4.6 Upgrade Firmware for Your Router

Before upgrading your router firmware, you need to install the Router Tools. The **Firmware Upgrade Utility** is included in the tools.

- 1. Insert CD of the router to your CD ROM.
- 2. From the webpage, please find out Utility menu and click it.
- 3. On the webpage of Utility, click **Install Now!** (under Syslog description) to install the corresponding program.

Please remember to set as follows in your DrayTek Router :

- Server IP Address : IP address of the PC that runs the Syslog
- Port Number : Default value 514

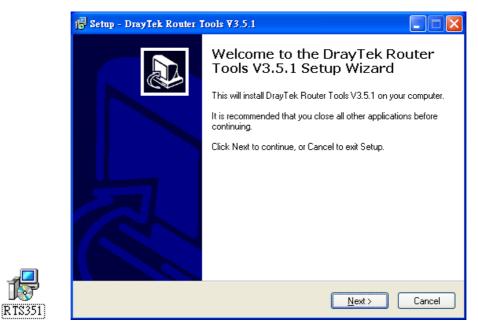
Install Now!

- 4. The file **RTSxxx.exe** will be asked to copy onto your computer. Remember the place of storing the execution file.
- 5. Go to www.draytek.com to find out the newly update firmware for your router.
- 6. Access into **Support Center** >> **Downloads**. Find out the model name of the router and click the firmware link. The Tools of Vigor router will display as shown below.

Tools Name	Released Date	Version	OS	Support Model	Download
Router Tools	21/12/2006	3.5.1	MS-Windows	All Model	zip
Smart VPN Client	18/08/2006	3.2.6	MS-Windows	All Model	zip
LPR	27/06/2005	1.0	MS-Windows	For Print Function	zip
VTA	15/09/2005	2.8	Windows2000/XP	For ISDN Model	zip
DialPlan	26/01/2006	2.5_lite	MS-Windows	For VoIP Model	zip

- 7. Choose the one that matches with your operating system and click the corresponding link to download correct firmware (zip file).
- 8. Next, decompress the zip file.

9. Double click on the icon of router tool. The setup wizard will appear.



- 10. Follow the onscreen instructions to install the tool. Finally, click **Finish** to end the installation.
- 11. From the **Start** menu, open **Programs** and choose **Router Tools XXX** >> **Firmware Upgrade Utility**.

៉ Firmware Upgrade	Utility 3.5.1	
Time Out(Sec.) 5	Router IP:	
Port	Firmware file:	
69 Password:		
	Abort	Send

- 12. Type in your router IP, usually **192.168.1.1**.
- 13. Click the button to the right side of Firmware file typing box. Locate the files that you download from the company web sites. You will find out two files with different extension names, **xxxx.all** (keep the old custom settings) and **xxxx.rst** (reset all the custom settings to default settings). Choose any one of them that you need.

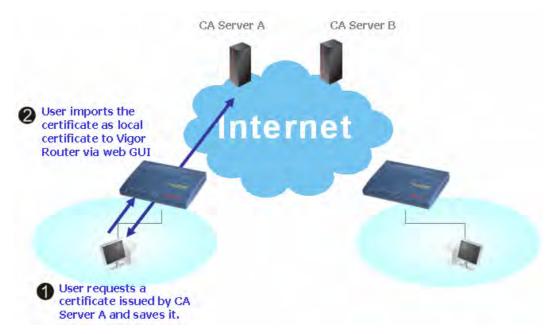
៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port 69	Firmware file: D:\ 5500 Series\VP5500_tw01.rst
Password:	Abort Send

14. Click Send.

៉ Firmware Upgrade	Utility 3.5.1
Time Out(Sec.) 5	Router IP:
Port	Firmware file:
69 Password:	D:\ 5500 Series\VP5500_tw01.rst
Can the s	Abort Send
Sending)

15. Now the firmware update is finished.

4.7 Request a certificate from a CA server on Windows CA Server



1. Go to Certificate Management and choose Local Certificate.

Certificate Management >> Local Certificate

lame	Subject	Status	Modify
.ocal			View Delete
	PORT REFRESH		
X509 Local Certific	ate		
			~

2. You can click **GENERATE** button to start to edit a certificate request. Enter the information in the certificate request. Certificate Management >> Local Certificate

Subject Alternative Name		
Туре	Domain Name 💌	
Domain Name	draytek.com	
Subject Name		
Country (C)	TW	
State (ST)		
Location (L)		
Orginization (O)	Draytek	
Orginization Unit (OU)		
Common Name (CN)		
Email (E)	press@draytek.com	
Кеу Туре	RSA 💌	
Key Size	1024 Bit 🔽	

- Generate
- 3. Copy and save the X509 Local Certificate Requet as a text file and save it for later use. Certificate Management >> Local Certificate

Local /C=TW/O=Draytek/emailAddress Requesting View Delete SENERATE IMPORT REFRESH X509 Local Certificate Request IMPORT REFRESH X509 Local Certificate Request IMIEGTOR CARTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAKGA1UEBhMCVFcxEDA0BgNVBAoTBORyYX102WsxIDAe BgkqhkiG9w0BCQEWEXby2Xn2QGRyYX102WsuY29tMIGfMA0GCSqGSIb3DQEBAQUA A4GNADCBiQKBgQDPioahu/gFQaYBIce50ERSDfWknIdHblo1kt9cTdLUDaFk6s8d 3wDeQytcV1LBJz2IDF0xjX61p7ev187twflsg41g260k/rGhuYTKd9j6PlcrnkP7 du84t23tWBdHD4W5c8VmSyDjShLbjdxVYPWpNKVIrOT2R2jkRMaHEWpVpwIDAQAB oCkwJWYUKo2IhvcNAQkOMkowGDAWBgWVHREEDzANgqtkcmF5dWrLmWvbTANBgkq hkiG9w0BAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToem1tHQbcwjXvg/t7kF1zTJ1Hh uRLqc1EiEnvAhmRytcx2pE268marSgRPEr86Ro083x0145560xC2/N1Gh9VQ911 IPFqkjJNihip4TCjecSNN2jmQoSWU+BceSTG+SCBCyjqu/fo/AJQFajB7Gviw= END CERTIFICATE REQUEST	Name	Subject	Status	Modify
X509 Local Certificate Request BEGIN CERTIFICATE REQUEST MIIBGJCCARMCAQAwGTELMAkGA1UEBhMCVFcxEDAOBgNVBAoTBORyYX102WsxIDAe BgkqhkiG9w0BCQEWEXByZXNzQGRYYX102WsuY29tHIGfNA0GCSqGSIb3DQEBAQUA A4GNADCB1QKBgQDPioahu/gFQaYB1ceS0ERSDfWknIdHb101kt9CTdLUDAFk668dd 3wDeQytoV1LBJz2IDF0xjXGip7ev187twwTsg41g26Qk/rGhuVTKd9j6P1crnkP7 du84c23tWBdHD4W5c8VmSyDjShLbjdxVYPWpNKVIrOT2R2jkRMaHEWpVpwIDAQAB oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq hk1G9w0BAQUFAA0BgQAuSBRUGt4W1hH9N6/HwToemItHQbcwJXvg(77kF1zT01Hh uRLq4C1E16074MRYtcz2p2E58marsgRREF66Ro08Jx0I45560xC2/NIGh9VQ911 19FqkjJN1hip4TCjecSNNZjmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==	Local	/C=TW/O=Draytek/emailAddress	Requesting	View Delete
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELNAkGA1UEBhMCVFcxEDAOBgNVBAoTBORyYX10ZWsxIDAe BgkqhkiG9w0BcQEWEXByZXNzQGRyYX10ZWsuY29tMIGfMA0GCSgGSID3DQEBAQUA A4GNADCBiQKBgQDPioahu/gFQaYBice5OERSDfWknIdHblo1kt9cTdLUDAFk6s8d 3wbeQytoVILBJz21DFOx}X6ip7ev187twwTsg4lg26Qk/ChuVTKd9j6PlcrnkP7 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2R2jkRMaHEWpVpwIDAQAB oCkwJwYJKoZIhvcNAQkOMRowcDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq hkG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToemItHQbcwjXvg17kF1zTJiHh ukLq4CiEi6nV4hMRytcxZp256sMarSgREEr66Ro08Jx0I45560xC2/NIGh9VQ9I1 I9FqkjJNihip4TCjecSNN2jmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==	GENERATE	IMPORT REFRESH		
MIIBqjCCARMCAQAwQTELNAkGA1UEBhMCVFcxEDAOBgNVBAoTBORYYX102WsxIDAe BgkqhkiG9w0BCQEWEXByZXN2QGRYX102WsuY29tMIGfMAOGC3qGSTh3DQEBAQUA A4GNADCBiQKBgQDPioahu/gFQaYBiceSOERSDfWknIdHblo1kt9cTdLUDaFk6s8d 3wbeQytoVILBJz2IDFOxjX6ip7ev187twwTsg4lg26Qk/r6huVTKd9j6PlcrnkP7 du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIrOT2RZjkRMaHEWpVpwIDAQAB oCkwJwYJKoZIhvcNAQkOMRowcDAWBgNVHREEDzANggtkcmF5dGVrLmNvbTANBgkq hkiG9w0BAQUFAAOBgQAuSBRUGt4WIhH9N6/HwToemItHQbcwjXvg/t7kFlzTJiHh ukLq4CiEi6nV4hMRvtcx2pE26sMarSgREEr66Ro83x0I455560xCZ/N1Gh9VQ9I1 I9FqkjJNihip4TCjecSNN2jmQo5WU+Bce8TG+SCBCyejqu/fo/AJQFajB7Gviw==	X509 Loc	al Certificate Request		
	MIIBqj(Bgkqhk: A4GNADO 3wDeQyt du84t23 oCkwJw3 hkiG9w0	CARMCAQAwQTELNAkGAIUEBhMCVFcxEDAO .G9wDBCQEWEXByZXN2QGRyYX10ZWsuY29t .BiQKBgQDPioahu/gFQaYB1ce50ERSDfWk .oV1LBJc2IDFOxjX6ip7ev187twwTsg41g ttWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVI JKoZIhvcNAQkOMRowGDAWBgMVHREEDAM)BAQUFAADBgQAuSBRUct4W1hHSN6/HwToe: .Ei6NV4hMRytcx2pE268MarSqRE186R00	MIGHNADGCSqGS nIdHblo1kt9cT Z6Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ BJx0I45560xCZ	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq v7kFlzTJiHh /NIGh9VQ9I1

4. Connect to CA server via web browser. Follow the instruction to submit the request. Below we take a Windows 2000 CA server for example. Select **Request a Certificate**.

Microsoft Certificate Services vigor <u>H</u>	lome
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, yo will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.	
Select a task:	
○ Retrieve the CA certificate or certificate revocation list	
Checks or a pending certificate	
Next >	

Select Advanced request.

Microsoft Certificate Services vigor	<u>Home</u>
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request.	
 Advanced request 	
	Next >

Select Submit a certificate request a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file

Microsoft Certificate Services - vigor	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the following methods. Note tha authority (CA) will determine the certificates that you can obtain.	t the policy of the certification
○ Submit a certificate request to this CA using a form.	
● Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #10 file or a	coded PKCS #7 file.
 Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station. You must have an enrollment agent certificate to submit a request for another user. 	

Import the X509 Local Certificate Requet text file. Select **Router (Offline request)** or **IPSec (Offline request)** below.

<i>Microsoft</i> Certilica Submit A Save	le Services - vigor d Request	Home
Paste a base64 server) into the n	and the second second second	r PKCS #7 renewal request generated by an external application (such as a web ntification authority (CA).
Saved Request:		
Certificate Request	EEGIN CERTIFICATE REQUEST- HIIEqjCCARNCAQAwQTELMAKGA1UEBhNCVFcs Bgkghki690BCCQWEXBZXNzQCRyX110ZMsi A4GNADCBiQKBgQDQYB7mmZFfFhN9/IeQnG03 hX4bp89cUF9dloACGGiM/tcBOckdcZdFFFv X/G0A7CTvO/fQ2pxroCw1JTjLSjS0/Bn9v50	11295 31k++ 1xcP3
	Browse for a file to insert.	
Certificate Templa	ite:	
	Administrator	
A statistics as	Administrator Authenticated Session Basic EFS EFS Recovery Agent	_
	User IPSEC (Offline request) Router (Offline request)	
	Subordinate Certification Authority Web Server	Submit >

Then you have done the request and the server now issues you a certificate. Select **Base 64 encoded** certificate and **Download CA certificate**. Now you should get a certificate (.cer file) and save it.

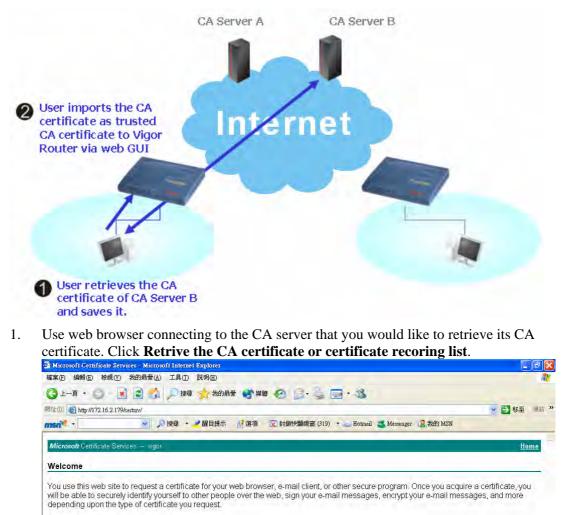
5. Back to Vigor router, go to **Local Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below window showing "-----BEGINE CERTIFICATE-----...." Certificate Management >> Local Certificate

ocal /C=TW/O=Draytek/emailAddress		
	Not Valid Yet	View Delete
NERATE IMPORT REFRESH		
X509 Local Certificate Request		
BEGIN CERTIFICATE REQUEST MIIBqjCCARMCAQAwQTELMAkGA1UEBhMCVFcxEDAOI BgkqhkiG9w0BCQEWEXByZXNzQGRyYX10ZWsuY29tJ A4GNADCBiQKBgQDPioahu/gFQaYB1ce50ERSDfWkn 3wDeQytoV1LBJz2IDF0xjX6ip7ev187twwTsg41g; du84t23tWBdMD4W5c8VmSyDjShLhjdxVYPWpNKVIn oCkwJwYJKoZIhvcNAQkOMRowGDAWBgNVHREEDzANg hkiG9w0BAQUFAAOBgQAuSBRUGt4W1hH9N6/HwToer uRLq4CiEi6nV4hMRytcxZpEZ6sMarSgRREr86RoOG I9FqkjJNihip4TCjecSNNZjmQoSWU+Bce8TG+SCB0 END CERTIFICATE REOUEST	MIGIMADGCSqGS nIdHblo1kt9cT Z6Qk/rGhuVTKd rOT2RZjkRMaHE ggtkcmF5dGVrL m1tHQbcwjXvg/ 8JxOI45560xCZ	Ib3DQEBAQUA dLUDaFk6s8d 9j6PlcrnkP7 WpVpwIDAQAB mNvbTANBgkq t7kFlzTJiHh /NIGh9VQ9I1

6. You may review the detail information of the certificate by clicking View button.

Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

4.8 Request a CA Certificate and Set as Trusted on Windows CA Server



Select a task:

Retrieve the CA certificate or certificate revocation list
O Request a certificate
O Check on a pending certificate

Vigor2910 Series User's Guide

Next >

- 2. In Choose file to download, click CA Certificate Current and Base 64 encoded, and Download CA certificate to save the .cer. file.
 - Microsoft Certificate Services Microsoft Internet Explored 檔案(P) 編輯(E) 檢視(Y) 我的最愛(A) 工具(I) 說明(H) 🌀 上一頁 • 🜍 - 📝 😰 🚮 🔎 搜尋 📩 我的最爱 🜒 媒體 🙆 🍙 è 🍃 🔜 • 🎕 網址 [D] Chttp://172.16.2.179/certsrv/certcarc.asp 🖌 🔁 移至 連結 msn. -💉 🔎 搜尋 • 🛃 醒目提示 🛃 選項 🔀 封鎖快顯視窗 (319) 🔹 🔤 Hotmail 👅 Messenger 👔 我的 MSN Retrieve The CA Certificate Or Certificate Revocation List Install this CA certification path to allow your computer to trust certificates issued from this certification authority. It is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the CA certification path will be installed for you automatically. Choose file to download: CA Certificate: Current [vigor(1)] Previous [vigor] Download CA certificate Download CA certification path Download latest certificate revocation list
- 3. Back to Vigor router, go to **Trusted CA Certificate**. Click **IMPORT** button and browse the file to import the certificate (.cer file) into Vigor router. When finished, click refresh and you will find the below illustration.

Certificate Management >> Trusted CA Certificate

Name	Subject	Status	Modify
Trusted CA-1	/C=US/CN=vigor	Not Yet Valid	View Delete
Trusted CA-2			View Delete
Trusted CA-3			View Delete

4. You may review the detail information of the certificate by clicking **View** button.

Name :	Trusted CA-1
Issuer :	/C=US/CN=vigor
Subject :	/C=US/CN=vigor
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

Close

Note: Before setting certificate configuration, please go to **System Maintenance** >> **Time and Date** to reset current time of the router first.

4.9 VPN TRUNK Application

You can change, disable or delete VPN TRUNK backup profile(s). Yet, the relational web pages in LAN-to-LAN also will be changed slightly. Please refer to the following expansion.

Change the name of VPN TRUNK profile(s)

- 1. Click any one of the items from Backup profile list.
- 2. Type a new name in the field of **Profile Name.**
- 3. Click Edit.

Disable VPN TRUNK profile(s)

- 1. Click any one of the items from Backup profile list.
- 2. Click **Disable** (as current status).
- 3. Click Edit.
- 4. The selected profile will be disabled.
- 5. To check if the profile has been disabled or not, open LAN-to-LAN. The name with red color means it has joined VPN TRUNK profile; the name with black color means it does not join VPN TRUNK profile or is disabled in VPN TRUNK profile.

AN-to-LAN Profiles:			LAN-to-LAN Profiles:		
Index	Name	Status	Index	Name	Status
<u>1.</u>	2.5	V	<u>1.</u>	2.5	V
2.	2.5-1	~	<u>2.</u>	2.5-1	V
<u>3.</u>	2.29	V	<u>3.</u>	2.29	V
4.	2.229	V	<u>4.</u>	2.229	V
<u>5.</u>	26	V	<u>5.</u>	2.2	V
6.	27	~	<u>6.</u>	27	V
Z.	28	V	<u>7.</u>	28	V
8.	29	v	<u>8.</u>	29	V
9.	30	V	<u>9.</u>	30	V

Delete VPN TRUNK profile(s)

- 1. Click any one of the items from Backup profile list.
- 2. Click Delete.
- 3. Click Edit.
- 4. The selected profile will be deleted.

Web Page Changes for VPN TRUNK

Corresponding web page (LAN-to-LAN) will be changed if VPN TRUNK is enabled. Refer to the following figures.

Dial-in call direction and Idle Timeout will be dimmish and cannot be used.

1. Common Settings	\frown
Profile Name 2.29	Call Direction 🛛 Both 💿 Dial-Out 🔍 Dial-In
Enable this profile	Always on
·	Idle Timeout 🛛 second(s)
VPN Connection Through: WAN1 Only 💌	Enable PING to keep alive
	PING to the IP

All the items in Allowed Dial-in Type will be dimmish and cannot be used.

Allowed Dial-In Type	
ISDN	Jsemeine
FPTP	Password
M IPSec Tunnel	VJ Compression @ Or @ Off
L2TP with IPSec Policy Must	IKE Authentication Method
Specify Remote VPN Gateway	Pre Shared Key
Feer VPN Server IP	IKE Pre-Shared Key
	Digital Signature(X.539)
cr Peer ID	None -
	IPSec Security Method
	Medum (AH)
	High (ESP)
	M DES M 3DES M AES
	Callback Function (CBCP)
	Enable Callback Function
	Use the Following Number to Callback
	Callback Number
	Callback Rudget 🛛 minute(s)

My WAN IP and Remote Gateway IP will be dimmish and cannot be used.

4. TCP/IP Network Settings	3	
My WAN IP	0.0.0.0	RIP Direction Disable 💌
Remote Gateway IP	0.0.0.0	From first subnet to remote network, you have to do
Remote Network IP	192.168.1.0	Route 💌
Remote Network Mask	255.255.255.0	
	More	☐ Change default route to this VPN tunnel (Only single WAN supports this)

In addition, after configuring VPN TRUNK profile(s), the Connection Management in VPN and Remote Access will be changed. Before adding a new VPN TRUNK profile, the webpage will be shown as the following:

VPN and Remote Access >> Connection Management

		Backup Mode: 🗾 🔽 Dial	/PN Connection Sta							
--	--	-----------------------	--------------------	--	--	--	--	--	--	--

After adding a new VPN TRUNK profile, it will be listed in Backup Mode drop-down list for you to choose for dialing.

VPN and Remote Access >> Connection Management

Dial-out Tool					Refres	sh Seco	onds :	10 💌 Refr	esh
	General Mo	ode: (2.2) 192.168.2.2		•	Dial			
	Backup Mo	ode: (Vp	nLB)192.168.2.10	3	•	Dial			
VPN Connection	Status								
Current Page: 1						Pa	ge No.[Go	>>
VPN T	ype Rei	note IP	Virtual Network	Tx Pkts	Tx Rate	Rx Pkts	Rx Rate	UpTime	

Examples for VPN TRUNK Backup Profile

Here provides two situations that you can take advantages of VPN TRUNK backup profile mechanism.

Example 1: A VPN TRUNK profile with member 1 (IPSec type) and Member 2(L2TP over IPSec) has been created for Router A for connecting with Router B. In general, Router A connects to Router B through Member 1 VPN tunnel (with IPSec type).

Backup profile list Set to Factory Default Note [Active:NO]The state may be Disable or Dial in Lan to Lan profile at present Member1(Active)Type 3(YES)IPSec Status Name v VpnBackup Member2(Active)Type 4(YES)L2TP over IPSec(MUST) No DIDBackup LITESTEET TESTEFT Status Enable O Disable Profile Name Member1 Please choose the combination that you want Please choose the combination that you want Member2
 Connection-Type>
 VPN ServerIP(Private Netw

 L2TP
 192.168.2.2(192.168.26.0)

 IPSec
 192.168.0.27(192.168.27.0)

 PPTP
 192.168.0.28(192.168.28.0)

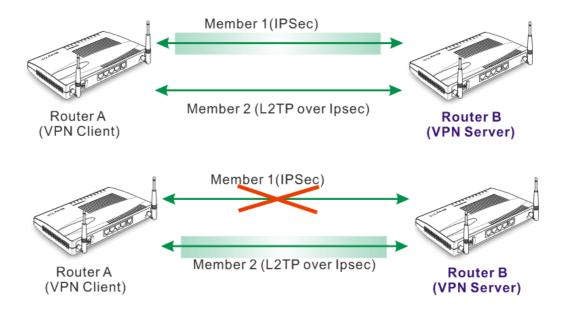
 L2TP over IPSec(NICE)192.168.0.29(192.168.29.0)
 L2TP over IPSec(NICE)192.168.0.30(192.168.30.0)

 L2TP over IPSec(NICE)192.168.0.31(192.168.31.0)
 L2TP over IPSec(NICE)192.168.0.31(192.168.31.0)

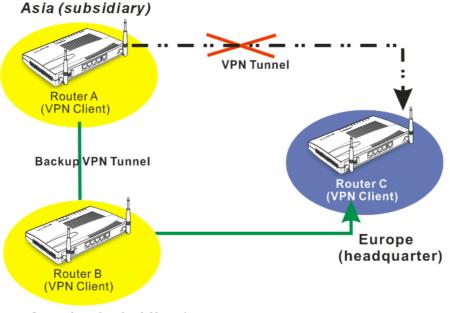
 L2TP over IPSec(NICE)192.168.0.31(192.168.31.0)
 L2TP over IPSec(NICE)192.168.0.31(192.168.31.0)
 <Name> 2.2 27 Network) No 5 Attribute Mode 6 28 29 8 9 10 30 31

VPN and Remote Access >> VPN TRUNK Management

However, if the connection is off-line, Router A will use Member 2 VPN tunnel (with L2TP over IPSec) instead to connect Router B right away.



Example 2: Subsidiary in Asia can use vigor router as VPN client. Every day it should transmit ERP, Mail or order information to headquarter in Europe. The Vigor router can build another backup VPN tunnel to subsidiary in America through LAN-to-LAN, and the VPN server in the subsidiary in American can build Routing /RIP. When the VPN tunnel is off-line, the subsidiary in Asia can send the data (that should be transmit to headerquarter in Europe) to the subsidiary in America, then the subsidiary in America transmit the data to headerquarter in Europe through VPN server by using VPN tunnel backup connection.

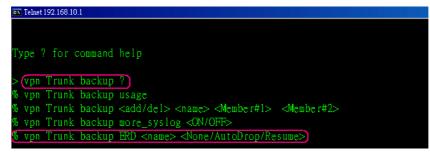


America (subsidiary)

4.10 ERD Mechanism for VPN TRUNK

To use ERD (Environment Recovery Detection) mechanism for VPN TRUNK, please follow the steps listed below:

- 1. Click **Start** >> **Run** and type **Telnet 192.168.1.1** in the Open box as below. Note that the IP address in the example is the default address of the router. If you have changed the default, enter the current IP address of the router.
- 2. Click OK. The Telnet terminal will be open. If an administrator password has not already been assigned, follow the on-screen instructions to assign one.
- 3. After assigning a password, type **?**. You will see a list of valid/common commands depending on the router that your use.
- 4. For using ERD mechanism, please type "vpn Trunk backup?". The available commands will be shown as the following figure.



(1) To inquire current ERD setting

```
> vpn Trunk backup ERD VpnBackup -----> (name of Trunk profile)
```

(2) None Mode (Default Setting)

Such mode makes all of the dial-out VPN TRUNK backup profiles being activated alternately.

Request Background: Some of users think if VPN tunnel connected again, it is Environment Recovery Detection. For such users, use None mode.

To set ERD None mode

> vpn Trunk backup ERD VpnBackup None

(3) Resume Mode

When VPN connection breaks down, Member1 is a top priority for the system to do VPN connection again.

Request Background: Some of users hope the connection can be continuous and not breaking down (maybe they will have thousands of orders coming within one minute). If the network connection breaks down, the users must connect from the first VPN server and spend lots of time. Such mode can solve their problems.

To set ERD Resume mode

> vpn Trunk backup ERD VpnBackup Resume

(4) AutoDrop Mode

Detect VPN connection periodically (by setting value for "second"). If VPN server for Member 1 has completed the network connection, current VPN Tunnel backup connection will be off-line.

Request Background: Some of users think it is not really environment recovery detection to borrow VPN tunnels from branches for connecting with the headquarters. The system should connect to headquarters automatically and that is called ERD.

To set ERD AutoDrop mode

To check current status of AutoDrop

>	vpn	Trunk	backup	ERD	VpnBackup	AutoDrop
		Го set Au	itoDrop			

> vpn Trunk backup ERD VpnBackup AutoDrop 3600

- Why use <second> AutoDrop might cause unstable condition for data transmitting. To solve the problem, you can set value for second to specify valid time for sending data out.
- When set value for <second> with "0": VPN tunnel that does not join Member1 will try to connect with VPN server of Member1 for every six seconds. Once the connection is successful, current transmitting data (mail, video conference, or other) will be dropped immediately.
- When set value for <second> with "1 ~ 4294967295": The administrator can try to connect with VPN server within certain time. Once the connection is successful, current transmitting data (mail, video conference, or other) will be dropped immediately. For example, if you type "3600" as the value for <second>, AutoDrop will be done with 30 seconds (3531 ~ 3600) for the backup VPN tunnel. If you set "30" as the value for <second>, it will be regarded as "0".

5 Trouble Shooting

This section will guide you to solve abnormal situations if you cannot access into the Internet after installing the router and finishing the web configuration. Please follow sections below to check your basic installation status stage by stage.

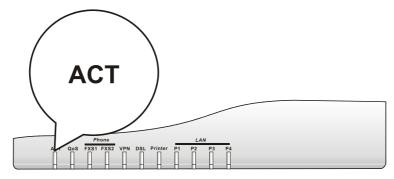
- Checking if the hardware status is OK or not.
- Checking if the network connection settings on your computer are OK or not.
- Pinging the router from your computer.
- Checking if the ISP settings are OK or not.
- Backing to factory default setting if necessary.

If all above stages are done and the router still cannot run normally, it is the time for you to contact your dealer for advanced help.

5.1 Checking If the Hardware Status Is OK or Not

Follow the steps below to verify the hardware status.

- 1. Check the power line and WLAN/LAN cable connections. Refer to "**2.1 Hardware Installation**" for details.
- 2. Turn on the router. Make sure the **ACT LED** blink once per second and the correspondent **LAN LED** is bright.



3. If not, it means that there is something wrong with the hardware status. Simply back to **"2.1 Hardware Installation"** to execute the hardware installation again. And then, try again.

5.2 Checking If the Network Connection Settings on Your Computer Is OK or Not

Sometimes the link failure occurs due to the wrong network connection settings. After trying the above section, if the link is stilled failed, please do the steps listed below to make sure the network connection settings is OK.

For Windows



The example is based on Windows XP. As to the examples for other operation systems, please refer to the similar steps or find support notes in **www.draytek.com**.

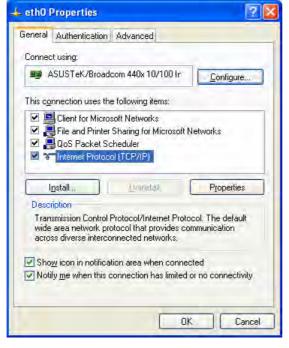
1. Go to Control Panel and then double-click on Network Connections.



2. Right-click on Local Area Connection and click on Properties.



3. Select Internet Protocol (TCP/IP) and then click Properties.



4. Select Obtain an IP address automatically and Obtain DNS server address automatically.

Internet	Protocol (TCP/IP)	Properties 🛛 🛛 🔀
General	Alternate Configuratio	n
this cap		ed automatically if your network supports need to ask your network administrator for
<u>O</u> D	otain an IP address auti	omatically
-O U <u>s</u>	se the following IP addr	855:
(Plac	ddress:	
Subr	iel mask	
Dela	ull gateway.	
0	gtain DNS server addre	ss automatically
OUs	se the following DNS se	erver addresses:
Erete	ared DNS server	
Alten	nate DNS server	
		Adyanced
		OK Cancel

For MacOs

- 1. Double click on the current used MacOs on the desktop.
- 2. Open the **Application** folder and get into **Network**.
- 3. On the **Network** screen, select **Using DHCP** from the drop down list of Configure IPv4.

		Network		
1 É		2		
now All Displa	vs Sound Network	Startup Disk		
	Location: A	utomatic	•	
	_			
	Show: B	uilt-in Ethernet	•	
	TCP/IP PPPoE	AppleTalk Pro	oxies Ethernet	
Configure	IPv4: Using DH	CP	•	
IP Ad	dress: 192.168.1	.10	(Renew DH	CP Lease
Subnet	Mask: 255.255.2	55.0 DHCP (Client ID:	
P	outer: 192.168.1	1	(If required)
K	Julei. 192.100.1			
DNS Se	rvers:			(Optional)
Search Dor	nains:			(Optional)
IPv6 Ad	lress: fe80:0000:	0000:0000:020a:95	off:fe8d:72e4	
	Configure	Pv6		(?)
				0

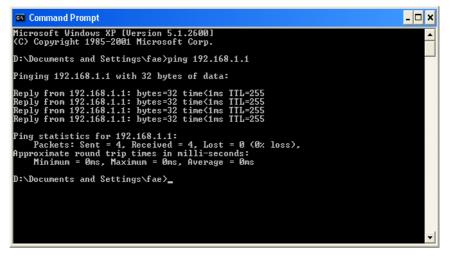
5.3 Pinging the Router from Your Computer

The default gateway IP address of the router is 192.168.1.1. For some reason, you might need to use "ping" command to check the link status of the router. **The most important thing is that the computer will receive a reply from 192.168.1.1.** If not, please check the IP address of your computer. We suggest you setting the network connection as **get IP automatically**. (Please refer to the section 4.2)

Please follow the steps below to ping the router correctly.

For Windows

- 1. Open the **Command** Prompt window (from **Start menu> Run**).
- 2. Type **command** (for Windows 95/98/ME) or **cmd** (for Windows NT/ 2000/XP). The DOS command dialog will appear.



- 3. Type ping 192.168.1.1 and press [Enter]. It the link is OK, the line of "**Reply from** 192.168.1.1:bytes=32 time<1ms TTL=255" will appear.
- 4. If the line does not appear, please check the IP address setting of your computer.

For MacOs (Terminal)

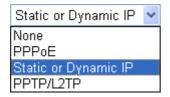
- 1. Double click on the current used MacOs on the desktop.
- 2. Open the Application folder and get into Utilities.
- 3. Double click **Terminal**. The Terminal window will appear.
- 4. Type **ping 192.168.1.1** and press [Enter]. It the link is OK, the line of **"64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**" will appear.

000	Terminal – bash – 80x24	
Welcome to Darwin! Vigor18:~ draytek\$ p PING 192.168.1.1 (19 64 bytes from 192.16 64 bytes from 192.16 64 bytes from 192.16 64 bytes from 192.16	02.168.1.1): 56 data bytes 08.1.1: icmp_seq=0 ttl=255 time=0.755 ms 08.1.1: icmp_seq=1 ttl=255 time=0.697 ms 08.1.1: icmp_seq=2 ttl=255 time=0.716 ms 08.1.1: icmp_seq=3 ttl=255 time=0.731 ms 08.1.1: icmp_seq=4 ttl=255 time=0.72 ms	2
5 packets transmitte	d, 5 packets received, 0% packet loss ax = 0.697/0.723/0.755 ms	

5.4 Checking If the ISP Settings are OK or Not

Click WAN>> Internet Access and then check whether the ISP settings are set correctly.

WAN >>	Internet Access		
Internet	Access		
Index	Display Name	Physical Mode	Access Mode
WAN1		Ethernet	Static or Dynamic IP 👻 🛛 Details Page
WAN2		Ethernet	None 🗸 Details Page



WAN >> Internet Access

For PPPoE Users

- 1. Check if the **Enable** option is selected.
- 2. Check if **Username** and **Password** are entered with correct values that you **got from** your **ISP**.

PPPoE Client Mode		PPP/MP Setup
🔘 Enable 🛛 💿 Disable)	PPP Authentication PAP or CHAP 💌
ISP Access Setup Username Password		Idle Timeout -1 second(s) IP Address Assignment Method (IPCP) WAN IP Alias
Password Index(1-15) in <u>Schedule</u> =>,,	≥ Setup:	Fixed IP: O Yes O No (Dynamic IP) Fixed IP Address
ISDN Dial Backup Setup Dial Backup Mode	None	 Default MAC Address Specify a MAC Address MAC Address:
WAN Connection Detectio	n	00 .50 .7F DD .15 .19
Mode	ARP Detect 💌	
Ping IP	0.0.0.0	
TTL:	255	

For Static/Dynamic IP Users

- 1. Check if the **Enable** option is selected.
- 2. Check if **IP address, Subnet Mask** and **Gateway** are entered with correct values that you **got from** your **ISP**.

WAN >> Internet Access

WAN 1

Static or Dynamic IP (D	HCP Client)	WAN IP Network Settin	gs WAN IP Alias	
💿 Enable i 🔘 Disal	ble	🔘 Obtain an IP addres	s automatically	
ISDN Dial Backup Setu	p	Router Name		*
Dial Backup Mode	None 💌	Domain Name * : Required for som	e ISPs	*
Keep WAN Connection		Specify an IP addre	ess	
Enable PING to kee	ep alive	IP Address	172.16.3.229	
PING to the IP		Subnet Mask	255.255.0.0	
PING Interval	0 minute(s)	Gateway IP Address	172.16.3.4	
WAN Connection Detec	tion	Oefault MAC Add	ress	
Mode	ARP Detect 💌	🔘 Specify a MAC A	ddress	
Ping IP	0.0.0.0	MAC Address:		
TTL:	255		. 15 . 19	
RIP Protocol		DNS Server IP Address	S	_
Enable RIP		Primary IP Address		
		Secondary IP Addre	ss	

5.5 Problems for 3G Network Connection

When you have trouble in using 3G network transmission, please check the following:

Check if USB LED lights on or off

You have to wait about 15 seconds after inserting 3G USB Modem into your Vigor2910. Later, the USB LED will light on which means the installation of USB Modem is successful. If the USB LED does not light on, please remove and reinsert the modem again. If it still fails, restart Vigor2910.

USB LED lights on but the network connection does not work

Check the PIN Code of SIM card is disabled or not. Please use the utility of 3G USB Modem to disable PIN code and try again. If it still fails, it might be the compliance problem of system. Please open DrayTek Syslog Tool to capture the connection information (WAN Log) and send the page (similar to the following graphic) to the service center of DrayTek.

		192.168.1.1	Getway IP (Static)	TX Packets	RX Rate
		DrayTek Vigor2910		-	0
AN Status				1 -	1 -
TX Packets	-	RX Packets	WAN IP (Static)	RX Packets	TX Rate
6442	I	3807	-	0	0
eWall Log VPN Log	z User Acce	ssLog Call Log WAN Lo.	g Network Infomation	Net State	
Time	Host	Message			0
Apr 12 09:17:49	Vigor	WAN2 PPPoE <== Protoco	ol:LCP(c021) ConfReq Ide	ntifier:0x03 ACCM: 0	0x0 Authe:
Apr 12 09:17:49	Vigor	[3G]Modem status:a1 20 0			
Apr 12 09:17:49	Vigor		ol:LCP(c021) ConfReq Ide	ntifier:0x00 MRU: 15	OO ACCM
Apr 12 09:17:49	Vigor	WAN2 PPPoE <== V:1 T:			
Apr 12 09:17:49	Vigor	[3G]Modem response: CO			_
Apr 12 09:17:49	Vigor	[3G]Modem status:a1 20 0			
	Vigor	[3G]Modem status:a1 20 0			
Apr 12 09:17:49					_
Apr 12 09:17:49	Vigor	[3G]Modem dial ATDT*9			
Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor	WAN2 PPPoE => V:1 T::	I PADR ID:0		-
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor	WAN2 PPPoE => V:1 T:: WAN2 PPPoE <= V:1 T::	I PADR ID:0 I PADO ID:0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor	WAN2 PPPoE => V:1 T:: WAN2 PPPoE <= V:1 T:: [3G]Modem response: OK	I PADR ID:0 I PADO ID:0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	WAN2 PPPOE => V:1 T: WAN2 PPPOE <= V:1 T: [3G]Modem response: OK [3G]Modem initialize AT&	I PADR ID:0 I PADO ID:0 &FE0V1X1&D2&C1S0=0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor	WAN2 PPPoE => V:1 T:: WAN2 PPPoE <= V:1 T:: [3G]Modem response: OK	I PADR ID:0 I PADO ID:0 &FE0V1X1&D2&C1S0=0		
Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49 Apr 12 09:17:49	Vigor Vigor Vigor Vigor Vigor	WAN2 PPPoE ==> V:1 T:: WAN2 PPPoE <== V:1 T:: [3G]Modem response: OK [3G]Modem initialize ATS WAN2 PPPoE ==> V:1 T::	I PADR ID:0 I PADO ID:0 &FE0V1X1&D2&C1S0=0		

Transmission Rate is not fast enough

Please connect your Notebook with 3G USB Modem to test the connection speed to verify if the problem is caused by Vigor2910. In addition, please refer to the manual of 3G USB Modem for LED Status to make sure if the modem connects to Internet via HSDPA mode. If you want to use the modem indoors, please put it on the place near the window to obtain better signal receiving.

5.6 Backing to Factory Default Setting If Necessary

Sometimes, a wrong connection can be improved by returning to the default settings. Try to reset the router by software or hardware.



Warning: After pressing **factory default setting**, you will loose all settings you did before. Make sure you have recorded all useful settings before you pressing. The password of factory default is null.

Software Reset

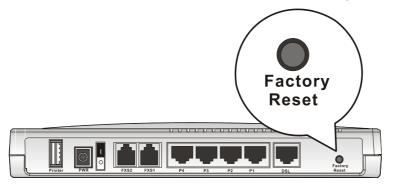
You can reset the router to factory default via Web page.

Go to **System Maintenance** and choose **Reboot System** on the web page. The following screen will appear. Choose **Using factory default configuration** and click **OK**. After few seconds, the router will return all the settings to the factory settings.

System Mainter	System Maintenance >> Reboot System					
Reboot System						
	Do You want to reboot your router ?					
	Osing current configuration					
	O Using factory default configuration					
1	ОК					

Hardware Reset

While the router is running (ACT LED blinking), press the **Factory Reset** button and hold for more than 5 seconds. When you see the **ACT** LED blinks rapidly, please release the button. Then, the router will restart with the default configuration.



After restore the factory default setting, you can configure the settings for the router again to fit your personal request.

5.7 Contacting Your Dealer

If the router still cannot work correctly after trying many efforts, please contact your dealer for further help right away. For any questions, please feel free to send e-mail to support@draytek.com.